ISSN 2363-1007

Commission européenne

Dix-septième rapport

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

Portant sur l'année 2013

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).

Dix-septième rapport du groupe de travail «Article 29» sur la protection des données — Portant sur l'année 2013
Commission européenne
Direction générale de la justice et des consommateurs
1049 Bruxelles
BELGIQUE

PDF ISBN 978-92-79-52065-5 ISSN 2363-1007 doi:10.2838/17385 DS-AA-15-002-FR-N

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, 2016

© Union européenne, 2016
Reproduction autorisée, moyennant mention de la source

Image de couverture: © robu_s / Fotolia.com

Dix-septième rapport du groupe de travail « Article 29 » sur la protection des données

Portant sur l'année 2013

Sommaire

AVANT-PROPOS DU PRÉSIDENT 2

QUESTIONS EXAMINÉES PAR LE GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES () 3

PRINCIPAUX DÉVELOPPEMENTS AU SEIN DES ÉTATS MEMBRES 17

- ALLEMAGNE 18
- AUTRICHE 22
- BELGIQUE 25
- BULGARIE 31
- CHYPRE 39
- CROATIE 41
- DANEMARK 43
- ESPAGNE 46
- ESTONIE 49
- FINLANDE 54
- FRANCE 58
- GRÈCE 66
- HONGRIE 72
- IRLANDE 79
- ITALIE 81
- LETTONIE 87
- LITUANIE 89
- LUXEMBOURG 92
- MALTE 95
- PAYS-BAS 98
- POLOGNE 102
- PORTUGAL 108
- RÉPUBLIQUE TCHÈQUE 110
- ROUMANIE 113
- ROYAUME-UNI 116
- SLOVAQUIE 121
- SLOVÉNIE 126
- SUÈDE 135

UNION EUROPÉENNE ET ACTIVITÉS COMMUNAUTAIRES 138

- 3.1. PARLEMENT EUROPÉEN 139
- 3.2. COMMISSION EUROPÉENNE 141
- 3.3. COUR DE JUSTICE DE L'UNION EUROPÉENNE 147

3.4. CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES 150

PRINCIPAUX DÉVELOPPEMENTS DANS LES PAYS DE L'EEE 156

ISLANDE 157

LIECHTENSTEIN 160

NORVÈGE 161

MEMBRES ET OBSERVATEURS DU GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES 165

MEMBRES DU GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES EN 2013 166

OBSERVATEURS DU GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES EN 2013 172

AVANT-PROPOS DU PRÉSIDENT

Suite à la présentation des propositions pour un nouveau cadre juridique au sein de l'Union européenne (UE) sur la protection des données en janvier 2012, le groupe de travail « Article 29 » a suivi la réforme de près et apporté en 2013 sa contribution à plusieurs sujets tels que les concepts de consentement, d'intérêt légitime, de limitation de la finalité et de profilage.

S'il est vrai, à l'heure de rédiger le présent avant-propos, que le Parlement européen a déjà adopté sa position sur ce programme, le Conseil continue d'en débattre. Néanmoins, en gardant à l'esprit le nouvel énoncé de mission de la Commission, il est raisonnable d'espérer que les négociations entre les différents législateurs de l'UE commenceront prochainement.

La réforme du cadre juridique de l'UE sur la protection des données a naturellement été l'un des principaux sujets sur lesquels le groupe de travail s'est concentré en 2013, mais n'a certainement pas été le seul sujet ayant nécessité l'attention des autorités européennes chargées de la protection des données. Lorsqu'Edward Snowden a révélé, pendant l'été 2013, que la NSA déployait des activités de surveillance à grande échelle et de manière systématique, et accédait à toutes les données (à caractère personnel) détenues ou passant par des entreprises basées aux États-Unis ou par le sol américain, le monde entier a réagi avec incrédulité et colère.

La nature extrême de ces révélations a provoqué l'indignation du public et engagé un dialogue critique entre l'UE et les États-Unis, auquel ont également participé le groupe de travail et les DPA nationales européennes. La quantité de données à caractère personnel des citoyens européens et la manière dont elles ont été consultées par les services de renseignements d'un pays tiers allié ont amené le groupe de travail à demander à la Commission européenne de s'engager avec les autorités américaines à corriger cette situation.

Le groupe de travail a par ailleurs adopté un avis traitant des principaux risques des applications mobiles pour la protection des données, détaillant les obligations spécifiques relevant du droit européen et applicables aux développeurs d'applications et à l'ensemble des parties impliquées dans le développement et la distribution des applications. Une attention particulière a été portée aux applications ciblant les enfants.

En 2013, le groupe de travail a également émis un avis sur la limitation de la finalité, dans lequel il a clairement établi que tout autre traitement à des fins différentes de celles pour lesquelles les données à caractère personnel sont recueillies au départ n'était pas nécessairement incompatible, mais que cette compatibilité devait être évaluée au cas par cas. Dans son avis, le groupe de travail offre des conseils sur l'application du principe en vertu de l'actuel cadre juridique ; néanmoins, il a aussi, en réponse aux discussions sur le principe de limitation de la finalité dans le cadre de la procédure d'examen, émis des recommandations applicables au futur cadre juridique général sur la protection des données.

Enfin, la protection des données n'est pas un sujet limité à l'UE, et le WP29 est resté en contact avec ses homologues du monde entier. La protection des données à caractère personnel est un objectif commun et une problèmatique de plus en plus globale. Ce n'est qu'en coopérant, entre nous et avec nos homologues à travers le monde, que nous serons en mesure d'assurer une protection adéquate à l'échelle internationale.

Jacob Kohnstamm

Chapitre Un
Questions examinées par le groupe de travail « Article 29 » sur la protection des données ([1])

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

1.1 TRANSFERT DE DONNÉES VERS DES PAYS TIERS

1.1.1 Règles d'entreprise contraignantes (*Binding Corporate Rules* – BCR)

19.04.2013 Document explicatif sur les règles d'entreprise contraignantes pour les sous-traitants – WP 204

Le présent document a vocation à donner des conseils sur l'application de l'article 26, paragraphe 2, de la directive 95/46/CE dans le cas des BCR pour les sous-traitants (au sein du même groupe d'entreprises), appliquée à compter du 1er janvier 2013, et à simplifier, pour les multinationales, le traitement et l'échange de données à caractère personnel au nom des responsables du contrôle à l'échelle internationale. Ce document de travail doit être considéré comme une première étape destinée à mettre en lumière la possibilité d'utiliser les BCR pour les sous-traitants sur la base d'une approche autorégulatrice et d'une coopération entre les autorités, sans préjudice de la possibilité d'utiliser, pour le transfert des données à caractère personnel à l'étranger, d'autres outils tels que les clauses contractuelles standard ou les principes de sphère de sécurité, le cas échéant.

1.1.2 Transferts à l'étranger à des fins spécifiques

4.4.2013 Lettre du groupe de travail « Article 29 » adressée à M. López Aguilar, de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, concernant la proposition d'une nouvelle directive de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)

Dans cette lettre, le groupe de travail fait part à la commission concernée du Parlement européen de ses inquiétudes quant à la législation LBC/FT. Le groupe de travail considère, entre autres, que la disposition relative à l'interdiction de divulguer l'existence d'une enquête constitue une limitation arbitraire des droits d'accès et de rectification. Il recommande de spécifier les opérations qui ne relèvent pas de cette interdiction, et oblige les autorités nationales de régulation et l'industrie à apporter les ajustements nécessaires.

Le groupe de travail recommande également de clarifier les conditions qui légitiment les transferts de données à caractère personnel à des fins de LBC/FT vers des pays tiers qui n'assurent pas un niveau adéquat de protection des données. Les États membres doivent spécifier quels intérêts publics importants s'appliquent au transfert des données en question vers le pays concerné et quelles garanties sont en place pour assurer une protection efficace des données.

Le groupe de travail conseille l'ajout de modalités plus spécifiques et/ou de garanties appropriées à chaque opération de profilage telles que le CDD, et encourage les parties prenantes à améliorer leur coopération dans le domaine de la protection des données, en faisant référence à l'exigence de contrôle préalable définie à l'article 20 de la directive 95/46/CE, ou à l'exigence d'évaluation de l'impact sur la vie privée définie à l'article 33 du projet de règlement.

13.6.2013 Procédure d'application finale uniforme et modèles standard pour les citoyens

Le groupe de travail, en conjonction avec les autorités des États-Unis, a développé pour les autorités de protection des données une application standard pour accéder à et/ou rectifier, effacer ou bloquer des données à caractère personnel détenues en vertu de la procédure prévue par le programme américain de surveillance du financement du terrorisme (TFTP), y compris la procédure uniforme détaillée faisant suite à une demande de la personne concernée d'avoir accès, de rectifier, d'effacer ou de bloquer des données à caractère personnel.

11.7.2013 Lettre adressée à Mme Cecilia Malmström, commissaire aux affaires intérieures, portant sur les informations anticipées sur les passagers (données API)

Cette demande du groupe de travail à la Commission répond à l'exigence selon laquelle les transporteurs aériens de l'UE doivent fournir des informations anticipées sur les passagers (données API) aux autorités des pays tiers de destination des vols concernés. Le groupe de travail n'est pas certain que ce type de transfert repose sur une base juridique existante, même si les données concernées sont fournies par les passagers à leur entrée dans le pays de destination, et, afin d'éliminer toute incertitude juridique et assurer la cohérence, il demande par conséquent à la Commission européenne de prendre des mesures pour introduire une base juridique spécifique.

Cette base juridique doit prévoir que les données devront être collectées et transférées uniquement si le droit du pays de destination l'exige ; elles devront être collectées et transférées par les compagnies aériennes à l'enregistrement uniquement aux fins du respect des obligations de contrôle aux frontières du pays tiers, et être supprimées sans délai une fois que l'avion a atteint sa destination finale ; la portée des données transférées doit se limiter aux information figurant dans la zone de lecture automatique du passeport ou autre document de voyage ; les données biométriques ne doivent pas être transférées ; les passagers doivent être informés du transfert avant d'acheter leur billet, ainsi que lorsque leurs données sont collectées.

Cette base juridique doit également prévoir des garanties adéquates pour les personnes concernées, y compris des modalités prévoyant l'exercice de leurs droits, et peut être introduite lors de l'évaluation et de la révision de la directive 2004/82/CE.

9.10.2013 Lettre du président du WP A29, Jacob Kohnstamm, aux membres du Comité LIBE concernant la proposition de décision du Conseil sur la conclusion de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement des données des dossiers passagers (données PNR)

Cette lettre donne l'avis du groupe de travail sur l'accord UE-Canada sur les données PNR. Le groupe de travail considère que la minimisation des données est de première importance pour la vie privée des passagers, et recommande que la nécessité de chaque élément figurant dans la liste de données soit examinée de manière distincte côté canadien. Le groupe de travail conseille également de réexaminer les définitions des termes prévention, détection, investigation et poursuites des infractions terroristes ou des formes graves de criminalité transnationale, actuellement trop vagues.

Le groupe de travail regrette que l'accord permette le traitement de données sensibles par les autorités canadiennes, et recommande que, dans le cas de violations de données ou d'incidents liés à la protection des données, les autorités européennes chargées de la protection des données concernées soient informées.

Concernant le contrôle de la mise en œuvre de l'accord, le groupe de travail suggère et recommande que les parties demandent aux transporteurs aériens de fournir aux passagers des informations sur les raisons, l'objectif, l'utilisation, le droit d'accès, le droit à l'information, les droits de correction et de recours relatifs au traitement de leurs données à caractère personnel.

Le groupe de travail suggère des références plus détaillées aux droits d'accès et de recours, et exprime son désaccord vis-à-vis de l'extension de la période de conservation par rapport à l'accord de 2005. Il suggère également que les autorités auxquelles les données peuvent être transférées figurent dans une liste jointe à l'accord ou ses annexes.

8.11.2013 Deuxième lettre du groupe de travail « Article 29 » adressée à M. López Aguilar, de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, concernant la proposition d'une nouvelle directive de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)

Par la voie d'un courrier en date du 8 novembre 2013, le groupe de travail a fait suite à cette lettre en réitérant des inquiétudes déjà soulevées qui n'avaient pas encore été prises en compte par les colégislateurs, selon lesquelles, notamment, les propositions n'étaient pas suffisamment spécifiques pour être considérées comme représentant une base juridique claire, contenaient de nouvelles mesures ne tenant pas compte de la vie privée et de la protection des données, et ignoraient la coopération avec les autorités de protection des données et le rôle de celles-ci.

5.12.2013 - Commentaires du groupe de travail « Article 29 » sur la question de l'accès direct par les services répressifs de pays tiers à des données stockées dans d'autres juridictions, comme proposé dans les projets d'éléments d'un protocole additionnel à la Convention de Budapest sur la cybercriminalité

Le sous-groupe ad-hoc du C-TY au Conseil de l'Europe sur la juridiction et l'accès transfrontalier aux données et aux flux de données a présenté des propositions visant à amender le protocole à la Convention de Budapest sur la cybercriminalité afin de permettre de nouvelles possibilités d'accès transfrontalier aux données, y compris d'accès transfrontalier sans consentement.

Le groupe de travail considère que, si le traitement des données à des fins répressives est légitime dans la mesure du respect du droit, compte tenu de l'importance croissante de l'informatique en nuage, avec la difficulté qui l'accompagne de lier les données à un lieu spécifique, et de l'absence de contrôle et de transparence inhérents au traitement des données de l'informatique en nuage, l'accès aux données à des fins répressives dans une autre juridiction constitue une violation des principes de la protection des données que sont la nécessité, la proportionnalité et la limitation de la finalité.

Par ailleurs, étant donné que les Conventions 108 et 185 du Conseil de l'Europe sont des conventions internationales, en cas de toute incompatibilité avec la Convention européenne des droits de l'homme, seuls les États européens seraient soumis à la juridiction de la Cour européenne des droits de l'homme, ce qui permettrait par conséquent son non-respect par les États non membres du Conseil de l'Europe.

11.12.2013 Lettre du groupe de travail « Article 29 » adressée à l'Association du transport aérien international (IATA) sur ses « nouvelles capacités de distribution »

Le groupe de travail a écrit à l'IATA afin de lui faire part de ses observations préliminaires sur les nouvelles capacités de distribution de l'IATA, et l'informer que la quantité de données à caractère personnel demandées doit être proportionnelle à l'objet du traitement, et que le traitement doit reposer sur une base juridique relevant de l'article 7 de la directive 95/46/CE.

Le groupe de travail a déclaré ne pas être certain que les critères de proportionnalité étaient respectés, ou qu'une base juridique fondée sur l'exécution d'un contrat était applicable dans le cas d'une demande de recherche générale non limitée à une compagnie aérienne en particulier. Ce traitement peut être basé sur un consentement libre, sans ambiguïté et explicite.

Les autres questions dont il convient de tenir compte comprennent le rôle des transporteurs eux-mêmes dans le cadre du processus de réservation, s'ils peuvent être considérés comme des responsables du traitement des données dans certaines circonstances à l'égard de la conservation des données, des informations aux passagers, des transferts potentiels vers des pays tiers en dehors de l'UE et des risques du profilage.

1.2 Communications électroniques, Internet et nouvelles technologies

27.2.2013 Avis 02/2013 sur les applications des dispositifs intelligents – WP 202

Dans cet avis, le groupe de travail clarifie le cadre juridique applicable au traitement des données à caractère personnel dans le développement, la distribution et l'usage des applications des dispositifs intelligents, en insistant sur l'exigence de consentement, les principes de limitation de la finalité et de minimisation des données, le besoin d'adopter des mesures de sécurité adéquates, l'obligation d'informer correctement les utilisateurs finaux de leurs droits, des périodes de conservation raisonnables et, plus spécifiquement, le traitement équitable des données collectées auprès et sur les enfants.

Cet avis conclut que de nombreux types de données disponibles sur un dispositif mobile intelligent sont des données à caractère personnel. Le cadre juridique correspondant est la directive 95/46/CE, associée à l'exigence de consentement spécifique visée à l'article 5, paragraphe 3, de la directive « Vie privée et communications électroniques ». Ces règles s'appliquent à toute application ciblant les utilisateurs de l'UE, quelle que soit la localisation du développeur ou de la boutique d'applications.

La nature fragmentée de l'écosystème applicatif, l'ampleur des possibilités techniques d'accéder aux données stockées dans ou générées par les dispositifs mobiles et l'absence de connaissances juridiques des développeurs créent pour les utilisateurs d'applications de nombreux risques graves en matière de protection des données. Ces risques vont de l'absence de transparence au manque de connaissances des utilisateurs d'applications, en passant par de mauvaises mesures de sécurité, des mécanismes de consentement non valides, une tendance à la maximisation des données et à l'élasticité de la finalité du traitement.

On observe un chevauchement des responsabilités en matière de protection des données entre les différentes parties participant au développement, à la distribution et aux capacités techniques des applications. La plupart des conclusions et des recommandations visent les développeurs d'applications (qui exercent le contrôle le plus important sur la manière précise dont le traitement a lieu ou dont les informations sont présentées dans l'application), mais souvent, dans le but de les inciter à renforcer leurs standards en termes de respect de la vie privée et de protection des données, ils doivent collaborer avec d'autres parties de l'écosystème applicatif, telles que les développeurs de systèmes d'exploitation et les fabricants de dispositifs, les boutiques d'applications et les tierces parties telles que les fournisseurs d'analyses et les réseaux publicitaires.

13.3.2013 Lettre du WP A29 adressée à Neelie Kroes, vice-présidente de la Commission européenne, sur la proposition de règlement de la Commission sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

Cette lettre fait part des inquiétudes du groupe de travail en matière de protection des données quant à la proposition de règlement de la Commission européenne sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Ces inquiétudes comprennent l'interprétation de certains termes utilisés dans la proposition, l'emploi de pseudonymes, la minimisation des données et les données à caractère personnel incluses dans les certificats, l'applicabilité de la directive 95/46/CE, les sceaux et les services de confiance électroniques, les signatures de masse et les signatures qualifiées pour les employés, l'identité électronique, la minimisation des données et le danger du profilage via les systèmes d'authentification et de validation en ligne, la sécurité des signatures électroniques, les autorités de contrôle, les listes de services de confiance qualifiés et les définitions des niveaux de sécurité.

18.6.2013 Lettre adressée à Google concernant Google Glass, un type d'ordinateur portable en forme de lunettes

Le groupe de travail a écrit à Google concernant Google Glass afin d'exprimer ses inquiétudes vis-à-vis du respect des lois sur la protection des données, des garanties de la vie privée, des informations collectées et de leur éventuel partage ultérieur, de l'objectif prévu pour les informations collectées, de la reconnaissance faciale, des questions sociales et éthiques plus larges soulevées, par exemple, par la collecte furtive d'informations sur d'autres personnes, et les résultats de toute évaluation des risques pour la vie privée.

2.10.2013 Document de travail 02/2013 fournissant des orientations sur l'obtention d'un consentement pour l'utilisation de cookies – WP 208

Depuis l'adoption de la directive 2002/58/CE « Vie privée et communications électroniques » amendée en 2009, plusieurs mises en œuvres pratiques ont été développées par les sites web afin d'obtenir le consentement pour l'utilisation de cookies à des fins diverses. Les différents mécanismes de consentement déployés par les opérateurs de sites web reflètent la diversité des organisations et de leurs types de public. L'opérateur de site web est libre d'utiliser différents moyens d'obtenir le consentement des internautes, dans la mesure où ledit consentement peut être considéré comme valide en vertu de la législation européenne. Cet avis évalue si oui ou non une solution particulière mise en œuvre par l'opérateur de site web respecte l'ensemble des exigences applicables à l'obtention d'un consentement valide.

Dans la pratique, la mise en œuvre des exigences légales varie parmi les opérateurs de sites web des différents États membres. En règle générale, ils s'appuient sur un certain nombre de pratiques, dont aucune ne pourrait à elle seule donner lieu à l'obtention d'un consentement valide.

Compte tenu des interprétations divergentes de la directive, l'avis clarifie les conditions à satisfaire pour que le consentement soit valide et ses principaux éléments, à savoir :

1. Spécificité des informations : le consentement doit être spécifique et reposer sur des informations appropriées, de sorte qu'un consentement général sans que soit spécifié exactement l'objet du traitement des données n'est pas acceptable.

2. Circonstance : le consentement doit être obtenu avant le début du traitement des données.

3. Choix actif : la procédure de demande et d'obtention du consentement ne doit laisser aucun doute quant à l'intention de la personne concernée. L'indication du souhait de l'utilisateur doit relever d'un choix actif.

4. Donné librement : le consentement ne peut être valide que si la personne concernée est en mesure d'exercer un véritable choix.

5. Si les opérateurs de sites web souhaitent s'assurer qu'un mécanisme de consentement pour l'utilisation de cookies respecte les conditions applicables dans chaque État membre, ledit mécanisme de consentement doit inclure chacun de ces éléments.

1.3 RÉVISION DU CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES

22.1.2013 Document de travail 01/2013 – Contributions sur les actes d'exécution proposés – WP 200

Dans ce document de travail, le groupe de travail explique les différences entre actes délégués et actes d'exécution tels qu'indiqués dans l'avis 8/2012, établit une liste des critères appropriés pour déterminer la justification et la nécessité des actes d'exécution et fournit une évaluation article par article de l'ensemble des actes d'exécution possibles.

26.2.2013Avis 01/2013 apportant des contributions supplémentaires sur les discussions relatives au projet de directive sur la protection des données dans les domaines de la police et de la justice pénale – WP 201

Dans cet avis, le groupe de travail fait part de ses commentaires sur le projet de directive du point de vue de l'utilisation des données des personnes non suspectes, des droits des personnes concernées, de l'utilisation d'analyses de l'impact sur la vie privée par les services répressifs, et des pouvoirs des autorités de protection des données.

27.2.2013 Déclaration du groupe de travail sur les discussions en cours concernant le programme de réformes sur la protection des données

Cette déclaration, qui fait suite aux avis WP 191 et WP 199 du groupe de travail, explique les inquiétudes soulevées précédemment dans les domaines de la flexibilité du secteur public, des données à caractère personnel et de la pseudonymisation, du consentement, de la gouvernance, des transferts internationaux et de l'approche fondée sur les risques. Les questions liées aux DPA « chefs de file », aux compétences et à l'exclusion des activités domestiques ou personnelles font l'objet de discussions encore plus approfondies.

Concernant la flexibilité du secteur public, le groupe de travail considère qu'une distinction entre les secteurs public et privé ne ferait qu'entrainer une incertitude juridique. Elle serait également impraticable en raison des différences existant d'un État membre à l'autre quant à la nature et l'étendue des tâches exécutées par les organismes publics.

La pseudonymisation des données implique de dissimuler l'identité de la personne concernée de manière à ce qu'elle soit réidentifiable. Dissimuler l'identité de manière à rendre toute réidentification impossible s'appelle l'anonymisation. Toutefois, lorsque la pseudonymisation ou le cryptage est effectué de manière à permettre le traçage ultérieur ou l'identification (indirecte) d'une personne, les règles de protection des données continuent de s'appliquer.

Dès lors que le consentement est destiné à servir de fondement juridique, il doit être suffisamment clair. Il peut être exprimé de nombreuses manières différentes, l'exigence essentielle étant qu'il soit explicite. Imposer la charge de la preuve du consentement au responsable du traitement renforce les droits des personnes.

Le renforcement des obligations du comité européen de la protection des données (CEPD) et des autorités de protection des données européennes améliorera la protection des données à caractère personnel, même s'il soulève la question de la disponibilité de ressources adéquates pour ces dernières. Les autorités devraient par ailleurs avoir la possibilité de définir leurs propres priorités et de prendre l'initiative d'actions telles que des enquêtes, nonobstant les obligations relatives à la coopération, l'assistance mutuelle et la cohérence.

Il est important que les données à caractère personnel des citoyens européens bénéficient de la même protection, qu'elles soient traitées au sein de l'UE ou transférées en dehors de l'UE. Les instruments non contraignants et l'auto-évaluation dans le contexte des transferts vers les pays tiers devraient rester une exception disponible uniquement dans des circonstances limitées et pour des transferts non massifs et non répétitifs. En cas de divulgation non autorisée par la loi, le recours aux traités d'entraide judiciaire doit être obligatoire.

Certaines dispositions du règlement proposé imposant la charge de la preuve à certains responsables du traitement peuvent être perçues comme inéquitables et devraient dès lors être adaptées au responsable du traitement et aux opérations de traitement concernées. La conformité doit porter sur la vérification que les données à caractère personnel sont suffisamment protégées, ce qui peut varier d'un responsable du traitement à l'autre. Cela dépend non seulement de la taille du responsable du traitement ou du volume du traitement, mais également de la nature du traitement et des catégories de données.

Annexe 1 : Propositions de modifications concernant les compétences et l'autorité de chef de file

Dans cette annexe, le groupe de travail délivre des propositions de modifications concernant les compétences et l'autorité de chef de file sur la base de l'obligation pour l'ensemble des autorités de contrôle d'être compétentes sur le territoire de leur État membre ; « l'autorité chef de file » doit être le seul point de contact d'une entreprise, s'occuper de la procédure décisionnelle à laquelle prendront part l'ensemble des autorités de contrôle concernées ; le résultat de la procédure décisionnelle doit être contraignant pour l'ensemble des autorités de contrôle ; la notion d'établissement principal doit être clarifiée et, s'il demeure une ambigüité quant à l'autorité qui doit jouer le rôle de « chef de file », une procédure décisionnelle doit être prévue, de préférence par le comité européen de la protection des données ; et les personnes doivent toujours avoir la possibilité d'obtenir une réparation judiciaire auprès des tribunaux de leur propre État membre.

Annexe 2 : Propositions de modifications concernant l'exclusion des activités domestiques ou personnelles

Dans cette annexe, le groupe de travail délivre des propositions de modifications concernant l'exclusion des activités domestiques ou personnelles en faisant référence aux critères qui permettent de décider si le traitement est effectué à des fins personnelles ou domestiques ; les autres éléments de la législation pertinents concernent la diffamation, le harcèlement, les communications malveillantes, l'incitation aux comportements menaçants et, dans certains cas, la persécution ou la discrimination, les intérêts lucratifs, le lien avec une activité professionnelle ou commerciale, le traitement personnel et la diffusion à travers le monde en général, et la correspondance et la conservation d'adresses.

13.5.2013 Document consultatif sur les éléments essentiels d'une définition et d'une disposition sur le profilage dans le cadre du règlement général de protection des données européen

Dans ce document, le groupe de travail présente ses conseils sur les éléments essentiels d'une définition et d'une disposition sur le profilage dans le cadre du projet de règlement général de protection des données, en prenant comme point de départ le fait que l'association de données à caractère personnel afin de créer des profils peut avoir des impacts importants sur la protection des données. Le profilage permet de déterminer, d'analyser et de prédire la personnalité ou les aspects liés à la personnalité d'une personne, le plus souvent sans que celle-ci n'en ait connaissance. Par conséquent, les personnes concernées peuvent ne pas être en mesure d'exercer un contrôle suffisant sur le traitement de leurs données à caractère personnel.

Le groupe de travail considère qu'il est nécessaire d'inclure une définition du profilage au règlement général de protection des données et propose une définition.

Le groupe de travail se prononce en faveur d'une approche qui permettrait de déterminer les conditions juridiques spécifiques, non seulement pour l'utilisation et le traitement ultérieur des données à caractère

personnel obtenues par la voie du profilage, mais également pour la collecte des données du profilage lui-même et la création de profils en tant que tel, et suggère d'y inclure d'autres éléments tels qu'une transparence et un contrôle individuel accrus quant à la décision d'autoriser ou non le traitement de ses propres données à caractère personnel à des fins de profilage ; le consentement explicite en tant que base juridique du traitement dans le contexte du profilage, ainsi que le droit d'avoir accès, de modifier ou d'effacer les informations de profil qui leur sont attribuées, et une plus grande responsabilisation des responsables du traitement quant à l'utilisation des techniques de profilage.

Le profilage devrait faire l'objet de mesures de protection des droits et libertés des personnes concernées, adoptées sur la base d'une évaluation de l'impact de la protection des données, et devrait inclure des technologies favorisant la protection des données et des paramètres par défaut standard, des mesures spécifiques pour la minimisation et la sécurité des données, ainsi que l'intervention de l'homme dans certains cas définis.

Étant donné que le profilage peut avoir différents effets sur la vie privée d'une personne, le règlement doit prévoir des règles claires sur la licéité et les conditions du traitement de données à caractère personnel dans le contexte du profilage, ce qui laisse une certaine latitude dans l'évaluation des effets réels d'un type spécifique de traitement sur les personnes concernées. Le groupe de travail soutient par conséquent une approche qui couvre le profilage sur ces bases, dans la mesure où il impacte de manière signficative les intérêts, les droits ou les libertés de la personne concernée. L'expression « impacte de manière signficative » doit être interprétée en tenant compte de l'étendue du droit fondamental à la protection des données, de l'évaluation des intérêts des responsables du traitement et de l'analyse des impacts potentiels des technologies de profilage sur les droits et les libertés des personnes concernées. La meilleure réponse à cette nécessité sera apportée par le comité européen de la protection des données.

1.4. DONNÉES À CARACTÈRE PERSONNEL

1.4.1 Limitation de la finalité

2.4.2013 Avis 03/2013 sur la limitation de la finalité – WP 203

Le présent avis vise à analyser le principe de limitation de la finalité, à donner des conseils sur l'application pratique du principe en vertu du cadre juridique applicable, et à formuler des recommandations stratégiques pour l'avenir. La limitation de la finalité protège les personnes concernées en fixant des limites à la manière dont les responsables du traitement de données peuvent utiliser leurs données, tout en offrant une certaine flexibilité aux responsables du traitement de données. Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes (spécification des finalités) et ne pas être traitées ultérieurement de manière incompatible avec ces finalités (compatibilité de l'utilisation).

La compatibilité doit être évaluée au cas par cas tout en tenant compte de toutes les circonstances applicables, et en faisant notamment référence à la relation entre la finalité de la collecte des données à caractère personnel et la finalité de tout traitement ultérieur, au contexte dans lequel les données à caractère personnel ont été collectées et les attentes raisonnables des personnes concernées quant à leur future utilisation, à la nature des données à caractère personnel, à l'impact de tout traitement ultérieur sur les personnes concernées et aux garanties adoptées par le responsable du traitement pour assurer l'équité du traitement, et prévenir tout effet indésirable sur les personnes concernées.

Le traitement de données à caractère personnel de manière incompatible avec les finalités déterminées lors de la collecte contrevient à la loi et est par conséquent interdit. Le responsable du traitement de données ne saurait légitimer un traitement incompatible en s'appuyant sur un autre fondement juridique

de l'article 7 de la directive 95/46/CE. Le principe de limitation de la finalité ne peut être restreint que par l'article 13 de la directive.

L'article 6, paragraphe 4, du règlement sur la protection des données proposé prévoit une large exception à l'exigence de compatibilité, qui pourrait gravement en restreindre l'applicabilité et le risque, et porter atteinte à ce principe clé. Le groupe de travail recommande par conséquent de supprimer le paragraphe 4 proposé et que les législateurs adoptent la liste ci-dessus des facteurs appropriés pour évaluer la compatibilité.

Avis 06/2013 sur la réutilisation des données ouvertes et des informations du secteur public (« ISP ») (416 ko) – WP 207 (5.6.2013)

Le présent avis concerne la directive 2003/98/CE modifiée concernant la réutilisation des informations du secteur public (la « directive ISP »), qui harmonise les conditions de réutilisation des informations du secteur public mais laisse le libre choix quant à la possibilité de mettre à disposition les données à des fins de réutilisation.

Son amendement avait pour objet de rendre toutes les informations publiques réutilisables à des fins tant commerciales que non commerciales, avec des exceptions portant, notamment, sur la protection des données.

La directive modifiée oblige désormais les organismes publics à autoriser la réutilisation de toutes les informations publiques accessibles au public en vertu du droit national et toujours sujettes à la loi sur la protection des données.

Une accessibilité accrue aux informations publiques entraîne certains risques. Pour minimiser ces risques, dès lors que la protection de la vie privée et des données à caractère personnel est en jeu, une approche équilibrée est nécessaire entre le développement du marché de la réutilisation d'un côté, et le droit à la protection des données à caractère personnel et de la vie privée de l'autre. Les données ouvertes ont plus vocation à renforcer la transparence et la responsabilisation des organismes du secteur public et la croissance économique que la transparence de chaque citoyen. Plutôt que des données à caractère personnel, ce sont souvent des données statistiques dérivées de données à caractère personnel qui sont et devraient être mises à disposition à des fins de réutilisation.

Dans certaines situations, les données à caractère personnel peuvent être réutilisées, dans la mesure du nécessaire, en vertu de mesures légales, techniques ou organisationnelles mises en place afin de protéger les personnes concernées. Dans ces cas, une base juridique claire, tenant compte des principes de proportionnalité, de minimisation des données et de limitation de la finalité, est nécessaire.

Le groupe de travail recommande que la possibilité d'informations contenant des données à caractère personnel soit prise en compte le plus tôt possible, conformément au principe de « protection des données dès la conception et par défaut » ; qu'une évaluation de l'impact de la protection des données soit effectuée avant d'autoriser la publication de données à caractère personnel ou de données anonymisées dérivées de données à caractère personnel ; lorsque des données sont anonymisées, il est essentiel d'évaluer le risque de réidentification, et il est de bonne pratique de tester la réidentification ; le résultat de l'évaluation peut contribuer à identifier les garanties appropriées pour minimiser les risques ou donner lieu à une décision de s'abstenir de publier et/ou de mettre à disposition des données à des fins de réutilisation ; les conditions de toute licence de réutilisation doivent inclure une clause de protection des données ; lorsque l'évaluation de l'impact conclut qu'une licence ne couvre pas les risques liés à la protection des données, les données à caractère personnel ne doivent pas être divulguées ; le cas échéant, les organismes du secteur public doivent s'assurer que les données à caractère personnel sont anonymisées et que les conditions de licence interdisent spécifiquement la réidentification des personnes et la réutilisation des données à caractère personnel à des fins susceptibles d'affecter les personnes concernées ; et les États membres doivent en outre envisager d'établir et d'apporter leur soutien aux réseaux de connaissances/centres d'excellence, ce qui permettrait de partager les bonnes pratiques liées à l'anonymisation et aux données ouvertes.

6.6.2013 Lettre du groupe de travail « Article 29 » adressée à l'ICANN concernant la déclaration sur l'impact de la révision du RAA de l'ICANN sur la protection des données

Dans cette lettre, le groupe de travail aborde la conformité de la proposition de convention régissant l'accréditation des bureaux d'enregistrement (RAA) finale de l'ICANN avec le droit européen sur la protection des données, traitant spécifiquement de la légitimité de l'obligation de conservation des données pour les bureaux d'enregistrement.

L'ICANN a inclus une procédure afin que les bureaux d'enregistrement demandent à être exonérés de ces exigences, si nécessaire, afin d'éviter une violation de la loi applicable sur la protection des données. Cette demande d'exonération peut être basée sur les indications écrites d'un organisme gouvernemental compétent, sous réserve que la conformité avec les exigences de conservation des données constitue une violation du droit applicable.

Le groupe de travail a observé que la nouvelle exigence de conservation des données proposée ne résultait d'aucune exigence juridique européenne, et a suggéré que, compte tenu de la diversité de ces bureaux d'enregistrement en termes de taille et de mesures de sécurité techniques et organisationnelles, et du risque de violations de données entraînant des effets indésirables pour les personnes détenant un nom de domaine, les risques pour la protection des données étaient disproportionnés par rapport aux avantages de la proposition.

Le groupe de travail a également contesté la conservation des données basée sur un contrat plutôt que sur le droit national, afin de répondre, par exemple, aux besoins sociaux pressants dans le cadre de l'application de la loi. Le fait que ces données à caractère personnel puissent être utiles à des fins répressives ne légitime par leur conservation au-delà de l'expiration du contrat.

1.4.2 Réseaux intelligents

Avis 04/2013 sur le modèle d'évaluation d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure, préparé par le groupe d'experts 2 de la task force sur les réseaux intelligents de la Commission (285 ko) – WP 205 (22.4.2013)

En 2012, la Commission européenne a publié une recommandation relative à la préparation de l'introduction des systèmes intelligents de mesure sur les marchés de l'électricité et du gaz (ci-après la « recommandation de la Commission ») afin, notamment, de conseiller les États membres sur les considérations liées à la protection des données. La Commission recommandait d'assurer la protection des données dès la conception et par défaut et préconisait que les États membres adoptent et appliquent un modèle d'évaluation d'impact sur la protection des données développé par la Commission et soumis à l'avis du groupe de travail.

Le groupe de travail en a conclu que, malgré les améliorations du modèle, un plus ample travail était nécessaire sur des questions telles que le champ d'application, les parties prenantes, le choix et la base juridique, la minimisation des données et les technologies renforçant la protection de la vie privée.

1.4.3 Frontières et Affaires intérieures

23.4.2013 Lettre du groupe de travail « Article 29 », adressée à l'IATA concernant le checkpoint du futur et annexe

Le groupe de travail a écrit à l'IATA concernant sa proposition de checkpoint du futur, lui indiquant qu'il soulevait des questions fondamentales sur sa conformité avec les règles de protection des données européennes et, plus particulièrement, les principes de nécessité et de proportionnalité, de qualité des données, de minimisation des données et de limitation de la finalité, les catégories particulières de données, la légitimité du traitement, les droits et la transparence vis-à-vis des personnes concernées, les décisions automatisées et le profilage, les transferts internationaux de données à caractère personnel et

la sécurité et la confidentialité des données. Le concept de vie privée dès la conception doit être un principe directeur, et les questions relatives à la vie privée doivent être prises en compte d'emblée.

L'annexe à cette lettre pose des questions spécifiques sur l'efficacité, la nécessité et la proportionnalité, la différenciation des passagers, le rôle des responsables du traitement de données et la conformité, la limitation de la finalité, les programmes de voyageurs connus, l'analyse des comportements, la transparence et l'accès des personnes concernées, la gestion des identités, le partage et l'accès aux données, et les technologies.

6.6.2013 Avis 05/2013 sur les frontières intelligentes – WP 206

En 2013, la Commission a présenté des propositions en faveur d'un système d'entrée/sortie (EES) et d'un programme d'enregistrement des voyageurs (RTP) à l'intérieur de l'espace Schengen, collectivement connus sous l'appellation de « frontières intelligentes ». Une proposition d'altérations nécessaires du code frontières Schengen a également été présentée.

La proposition de système d'entrée/sortie propose un système centralisé de stockage pour l'entrée et la sortie des données relatives à l'entrée et à la sortie des ressortissants de pays tiers admis pour de courts séjours à l'intérieur de l'espace Schengen, qu'ils requièrent un visa Schengen ou non. Plutôt que de devoir tamponner les passeports à l'entrée et à la sortie de l'espace Schengen, les données relatives à l'identité du visiteur, à la durée et à l'objet de son séjour seront saisies dans le système à son entrée et vérifiées à sa sortie afin de s'assurer que les citoyens de pays tiers ne dépassent pas la durée maximale de séjour autorisé. Un système centralisé signifie que les données EES peuvent être contrôlées de n'importe quel point de sortie de l'espace Schengen choisi par un citoyen d'un pays tiers. Le principal objectif de ce système est de mettre un terme au problème du dépassement de la durée de séjour autorisé au sein de l'espace Schengen. La proposition EES porte sur un système initialement basé sur les données à caractère personnel nécessaires à l'identification des personnes (données alphanumériques), les données biométriques n'ayant vocation à être introduites qu'après trois ans. Au-delà de deux ans, une évaluation est prévue sur l'opportunité d'ouvrir l'accès au système aux services répressifs et aux pays tiers.

Le programme d'enregistrement des voyageurs (RTP) propose un enregistrement volontaire des voyageurs qui se rendent fréquemment dans l'espace Schengen, tels que les voyageurs d'affaires, par exemple. Les citoyens de pays tiers peuvent demander le statut de voyageur enregistré et bénéficier d'un passage plus rapide à la frontière. Le RTP sera basé sur un registre central contenant des données biométriques et un jeton contenant un numéro d'identification unique pour chaque voyageur.

Le présent avis demande si l'EES pourra atteindre efficacement ses propres objectifs déclarés. Toutefois, même s'il était accepté que l'EES présentait une importante valeur ajoutée, il a été conclu que la valeur ajoutée du système dans la réalisation de ses objectifs déclarés n'atteignait pas le seuil de nécessité susceptible de justifier des interférences avec les droits prévus à l'article 8 de la Charte européenne. Il a par ailleurs été exprimé que la valeur ajoutée de l'EES n'était pas proportionnelle à l'échelle de son impact sur les droits fondamentaux liés à chacun de ses objectifs et qu'il existait des alternatives pour les atteindre.

9.12.2013 Lettre du groupe de travail « Article 29 » adressée à M. López Aguilar, de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, concernant la proposition de règlement du Parlement européen et du Conseil sur EUROPOL

Dans cette lettre, le groupe de travail commente la proposition de règlement de la Commission européenne sur une agence de l'Union européenne pour la coopération et la formation des services répressifs (règlement Europol), sur lequel le Contrôleur européen de la protection des données (CEPD) et l'autorité de contrôle commune (ACC) d'Europol ont déjà adopté des avis.

Le groupe de travail considère que le niveau de protection des données, tel que défini dans la proposition, ne répond pas aux normes visées par la décision Europol du Conseil, et que la proposition

doit être améliorée pour contribuer à un régime de protection des données amélioré et renforcé pour Europol. C'est la raison pour laquelle il semble nécessaire de reformuler certaines dispositions clés du projet de règlement Europol et d'introduire, dans la mesure du possible, des garanties de protection des données renforcées et spécifiques aux activités d'Europol.

Le groupe de travail considère qu'il convient de définir et de décrire plus précisément l'étendue des compétences d'Europol ainsi que les crimes spécifiques pour lesquels Europol sera compétent à l'avenir.

Les responsabilités relatives aux informations fournies par des tierces parties ne sont pas clairement établies, et les responsabilités liées aux résultats des analyses réalisées par Europol ne sont pas non plus clairement attribuées. Compte tenu du lien entre les données utilisées pour préparer un rapport et le résultat final, tout rapport basé sur des données imprécises devra être mis à jour en conséquence, ce qui ne pourra être fait que lorsqu'une responsabilité aura clairement été attribuée.

Les dispositions relatives aux finalités des activités de traitement des informations ne semblent pas permettre à Europol d'exécuter ses tâches présentes et futures, et auront un impact négatif sur la vie privée des personnes. Il convient de définir les conditions de création des systèmes de traitement de données où seules des données à caractère personnel spécifiques devront être traitées. La proposition bénéficierait de l'ajout d'éléments spécifiques au respect de la vie privée dès la conception, c'est-à-dire de l'inclusion d'analyses de l'impact sur la vie privée en tant qu'outil obligatoire dans certains cas spécifiques, ainsi que de mécanismes assurant le respect de la vie privée par défaut.

Le groupe de travail note l'absence d'une obligation de notifier les violations de données à caractère personnel à l'autorité de contrôle et à la personne concernée dans certains cas spécifiques, pourtant incluse dans le paquet de propositions pour la protection des données et, notamment, les articles 28 et 29 de la directive proposée. Le groupe de travail recommande d'inclure cette obligation à la proposition en tenant compte des spécificités des tâches d'Europol.

1.4.4 Sports

5.3.2013 Lettre du groupe de travail « Article 29 » adressée à l'Agence mondiale antidopage concernant la 3e phase de la consultation de l'AMA dans le contexte de l'examen du Code mondial antidopage et de ses normes internationales, et contribution annexe

Suite à ses avis WP 156 et WP 162 en 2008 et 2009, portant respectivement sur le Standard international pour la protection des renseignements personnels, sur certaines dispositions pertinentes du Code mondial antidopage et des standards de contrôle, le groupe de travail a supervisé le processus de révision du Code mondial antidopage et, dans le contexte de la troisième et dernière phase de la consultation publique organisée par l'AMA, a exprimé, avec cette lettre, un certain nombre d'observations et d'inquiétudes liées principalement aux questions de légitimité basée sur le consentement, de proportionnalité des données de localisation, des périodes de conservation et (des conditions) de publication automatique des sanctions, ainsi qu'à l'adéquation du cadre applicable aux transferts internationaux de données.

1.4.5 Surveillance

18.4.2013 Lettre du groupe de travail « Article 29 » adressée à l'INDECT

Le groupe de travail à écrit au coordinateur du projet INDECT, un projet de recherche financé par la Commission, en réponse à une explication du projet INDECT donnée au groupe de travail l'année précédente. Le groupe de travail a clarifié que, le plus souvent, les enregistrements vidéo devaient être considérés comme des données à caractère personnel en raison de leur nature particulière, et a fourni à l'INDECT un bref aperçu de ce qui devait être considéré comme des données à caractère personnel.

Le groupe de travail a reconnu que le projet INDECT avait obtenu le consentement de toutes les personnes impliquées dans les recherches, mais a suggéré que lorsque le projet de recherche nécessitait

le traitement de données à caractère personnel et était susceptible d'affecter la vie privée de citoyens européens, non seulement les recherches elles-mêmes et la manière dont elles étaient entreprises, mais également les résultats des recherches, devaient respecter les droits fondamentaux et, plus particulièrement, le droit à la vie privée et à la protection des données, avant le déploiement pratique des résultats.

Le groupe de travail a suggéré des considérations proactives telles que les principes de « minimisation des données », de « respect de la vie privée dès la conception » et de « protection des données par défaut » dans le développement des nouvelles technologies et solutions, appréciant que de nombreuses technologies visant à détecter les menaces potentielles focalisaient l'attention des agents de sécurité ou de surveillance sur de possibles événements dangereux via « d'innovants algorithmes d'aide à la décision humaine » qui n'avaient pas besoin d'identifier les personnes présentes dans les enregistrements vidéo.

Le groupe de travail a attiré l'attention de l'INDECT sur les risques pour la vie privée et la sécurité des données associés à la nature des recherches entreprises.

Chapitre Deux
Principaux développements au sein des États membres

ALLEMAGNE

A. Résumé des activités et actualités

Commissaire fédéral à la protection des données et à la liberté de l'information

Veuillez noter ce qui suit : En Allemagne, le commissaire fédéral à la protection des données et à la liberté de 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 des Länder, et la Bavière possède en outre une autorité de contrôle distincte dédiée au secteur privé.

Le tableau ci-dessous fait uniquement référence au bureau du commissaire fédéral à la protection des données et à la liberté de l'information.

Organisation	Commissaire fédéral à la protection des données et à la liberté de l'information
Président et/ou collège	M. Peter Schaar (jusqu'au 17 décembre 2013) et Mme Andrea Voßhoff[2]
Budget	9 090 000 €
Personnel	85
Activités générales	
Décisions, avis, recommandations	-
Notifications	-
Contrôles préalables	-
Demandes émanant de personnes concernées	12 074
Plaintes émanant de personnes concernées	Aucune distinction n'est faite entre les plaintes et les demandes
Conseils sollicités par le Parlement ou le gouvernement	-
Autres renseignements relatifs aux activités générales	-
Activités d'inspection	
Contrôles, enquêtes	104
Activités de sanction	

[2] Mme Andrea Voßhoff a été élue en tant que nouvelle commissaire fédérale à la protection des données et à la liberté d'information par le Parlement fédéral allemand le 19 décembre 2013, fonction qu'elle occupe depuis sa nomination le 6 janvier 2014.

Sanctions	-
Amendes	0
DPD	
Chiffres relatifs aux DPD	-

Pendant la période de référence, aucune évolution ou changement important de la situation de la protection des données n'a été observé en Allemagne sur le plan législatif.

La proposition de l'OCDE en faveur d'un système mondial d'échange d'informations pour lutter contre la fraude et l'évasion fiscales est un exemple, décrit plus en détail ci-dessous, d'évolution au niveau international qui a des incidences sur la mise en œuvre au niveau national.

La crise financière mondiale, les scandales impliquant les CD de données fiscales et la délocalisation croissante de biens privés à l'étranger ont amené le G20, l'OCDE, le Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales et l'UE à prendre, sur le plan international, des mesures décisives contre la fraude et l'évasion fiscales.

Le 20 juillet 2013, les ministres des finances et les gouverneurs des banques centrales du G20 ont approuvé une proposition de l'OCDE en faveur d'un modèle mondial d'échange automatique dans un cadre multilatéral. La décision du G20 doit également être envisagée dans le contexte de la décision unanime du Conseil européen du 22 mai 2013, qui a donné la priorité à l'expansion de l'échange automatique d'informations aux niveaux européen et mondial.

Le 13 février 2014, l'OCDE a présenté une norme mondiale d'échange automatique d'informations. Celle-ci spécifie les informations qui doivent être partagées ainsi que les prestataires de services financiers et les contribuables qui sont couverts. Cette norme internationale comprend un modèle d'accord, une norme commune de déclaration, des commentaires sur l'interprétation et des normes minimales pour les solutions informatiques.

Une période allant jusqu'à mi-2014 est envisagée pour élaborer les commentaires relatifs à cette norme. Le ministère fédéral des finances a introduit la clause de protection des données allemande, qui comprend des références à des peines privatives de liberté et à la peine capitale, dans la discussion. Le modèle mis au point par l'OCDE repose en grande partie sur une approche intergouvernementale de la mise en œuvre de la loi relative au respect des obligations fiscales concernant les comptes étrangers (dite « loi FATCA ») initiée par les États-Unis.

Le G5 a accepté d'introduire la norme avant la fin de l'année 2015 (FATCA plus un an et demi). Cela signifie qu'à compter du 31.12.2015, les établissements financiers devront examiner leurs données relatives à des comptes existants détenus par des résidents fiscaux d'autres états et, à compter du 01.01.2016, devront enquêter sur la résidence fiscale des titulaires de comptes conformément à un processus prescrit (procédure de diligence raisonnable). Le premier rapport sera adressé à l'administration fédérale des impôts en septembre 2017. Dans le cadre de la révision de la directive relative à l'assistance administrative, la Commission européenne vise à mettre en œuvre le modèle d'accord entre autorités compétentes et la norme commune de déclaration (accord AAC/NCD) au sein de l'UE, sans toucher au contenu du cadre législatif européen.

Le ministère fédéral des finances estime qu'un accord AAC/NCD devrait être appliqué au niveau national par voie de règlement, afin d'en simplifier la promulgation. L'autorisation légale requise pour ce faire devrait en déterminer précisément le contenu, la finalité et le champ d'application conformément à l'article 80(1) de la loi fondamentale allemande. La section 117c du code allemand des impôts ne satisfait pas à cette exigence parce qu'elle fait référence à un accord international transposé en droit

national et que l'accord AAC/NCD n'est qu'un accord administratif. Pour des raisons de protection de données en particulier, une base légale spécifiée de manière précise est toutefois requise pour l'échange automatique d'informations. L'objectif est par conséquent d'ajouter au code allemand des impôts une section 117d qui définirait précisément les informations à échanger ainsi que la finalité et le champ d'application de l'utilisation de ces informations.

Cette disposition devra tenir compte du principe de finalité. Par ailleurs, une garantie de sécurité adéquate des données devra être fixée par la loi en ce qui concerne l'échange automatique d'informations. La forme de la garantie des droits de protection de données des personnes concernées doit encore être clarifiée. Il est ici possible d'intégrer une disposition à la loi d'habilitation ou au règlement. Il est essentiel pour la structure qui sera déployée que la personne concernée dispose d'informations suffisamment transparentes sur ses droits en tant que personne concernée.

Le commissaire fédéral à la protection des données et à la liberté d'information (BfDI) a clairement établi, dans le cadre de sa réponse au ministère fédéral des finances, que le déploiement national de l'accord AAC/NCD pour mettre en œuvre la nouvelle norme élaborée par l'OCDE pour favoriser l'échange automatique d'informations, portait atteinte au droit à l'autodétermination informationnelle visée à l'article 2(1) en conjonction avec l'article 1(1) de la loi fondamentale, et nécessitait par conséquent une base juridique proportionnée répondant à l'exigence constitutionnelle de clarté des règles juridiques.

La mise en œuvre de l'accord AAC/NCD, qui est classé par le ministère fédéral des finances en tant qu'accord administratif en vertu du droit international selon la deuxième phrase de l'article 59(2) de la loi fondamentale, doit respecter le cadre de l'autorisation légale, qui reste dans ce cas à créer. Il convient de porter ici une attention suffisante au besoin de clarté de l'instrument spécifique Par exemple, selon l'article 80(1), deuxième phrase, de la loi fondamentale, le contenu, la finalité et la portée du pouvoir conféré doivent être spécifiés dans la loi d'habilitation. Le commissaire fédéral a convenu avec le ministère fédéral des finances qu'une base juridique distincte (section 117d du code allemand des impôts) était nécessaire pour satisfaire aux exigences de protection de données.

B. Informations sur la jurisprudence

Trois décisions de justice traitant, notamment, de l'applicabilité du droit allemand à des opérateurs Internet étrangers, ont été rendues en 2013. L'évaluation a révélé plusieurs contradictions, notamment les décisions suivantes :

Tribunal régional de Berlin, 30.04.2013 (réf. 15 O 92/12)

En examinant le contenu des lignes directrices sur la protection des données d'Apple Sales International, Irlande, en vertu du Code civil allemand, le tribunal a vérifié les clauses appliquées par la société en matière de traitement des données à caractère personnel. Les dispositions de la loi fédérale sur la protection des données ont servi de critères d'examen.

Cour fédérale de justice, 14.05.2013 (réf. VI ZR 269/12)

La Cour a statué sur la demande d'une partie lésée demandant la suppression de suggestions spécifiques d'un moteur de recherche (la fonction « saisie semi-automatique ») qui constituaient, selon elle, une violation des droits de protection de la vie privée, contre l'opérateur américain de moteur de recherche Google.

3. Tribunal administratif supérieur de Schleswig, 22.04.2013 (réf. 4 MB 11/13)

Dans une décision non contestable, la Cour a conclu que seule la législation irlandaise sur la protection des données s'appliquait au traitement des données par Facebook Ireland Limited et ce, même pour les utilisateurs allemands, plutôt que le droit allemand. Cette décision a été rendue aux motifs que Facebook Ireland Ltd. est une filiale de Facebook en Europe.

C. Autres informations importantes

Suite à la divulgation publique des activités de surveillance des États-Unis et du Royaume-Uni, le commissaire fédéral à la protection des données et à la liberté de l'information les a invités à une réunion du comité des affaires internes l'été dernier. Pendant cette réunion, d'importantes questions liées à la protection des données ont été évoquées.

Le commissaire a également adressé une déclaration écrite sur ces questions à tous les membres du Parlement en vue d'une audience prévue en novembre 2013. Cette déclaration a été incluse à la documentation officielle du Parlement (BT Drs. 18/59). L'opinion pourrait être ainsi sensibilisée aux questions de protection des données.

AUTRICHE

A. Résumé des activités et actualités

Sur la période de référence, le Parlement a adopté l'**amendement 2014 de la loi sur la protection des données (DSG)**[3]. Celui-ci exige la création d'une **autorité monocratique de protection des données** afin de remplacer la Commission de protection des données. Un processus d'appel de l'autorité de protection des données devant le tribunal administratif fédéral (lui-même établi en 2014) est également envisagé.

La Commission de protection des données a par conséquent cessé ses activités d'autorité de contrôle en matière de protection des données, telles que visées à l'article 28 de la directive sur la protection des données[4] le 31.12.2013.

Organisation	Commission autrichienne de la protection des données
Président et/ou collège	Président : Dr Anton SPENLING Membre administrateur : Dr Eva SOUHRADA-KIRCHMAYER Membres du collège : Dr Anton SPENLING, Dr Eva SOUHRADA-KIRCHMAYER, M. Helmut HUTTERER, Dr Claudia ROSENMAYR-KLEMENZ, Dr Klaus HEISSENBERGER, Mme Daniela ZIMMER.
Budget	Pas de budget propre en 2013. Les dépenses sont couvertes par le budget de la Chancellerie fédérale.
Personnel	16 postes à temps plein et 8 à temps partiel (21,85 équivalents temps plein)
Activités générales	
Décisions, avis, recommandations	107 décisions formelles (plaintes), 326 dossiers déposés auprès du médiateur et 49 autorisations (transfert de données vers des pays tiers, recherche et enquêtes).
Notifications	11 404
Contrôles préalables	4 193
Demandes émanant de personnes concernées	Par écrit : 1 136 Par téléphone : aucune documentation écrite, jusqu'à 100 appels par jour
Plaintes émanant de personnes concernées	Plaintes ayant mené à une décision formelle : 107 Plaintes ayant mené à un éclaircissement ou à une recommandation : 326
Conseils sollicités par le Parlement ou le gouvernement	Cette fonction relève de la compétence de deux autres institutions : le « Datenschutzrat » (conseil de la protection des données) et le

[3] Journal officiel fédéral (BGBl.) I Nº 83/2013.

[4] 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.

	service juridique du gouvernement, qui dépend de la Chancellerie fédérale.
Autres renseignements relatifs aux activités générales	160 millions d'identifiants spécifiques à des secteurs ont été émis, plus de 10 000 nouvelles personnes, environ 1,4 million de nouvelles personnes morales ont été inscrites au registre des identités électroniques et 546 mandats électroniques ont été authentifiés par l'autorité d'enregistrement de l'administration en ligne, qui fait partie de la DPA autrichienne. Cette autorité est responsable de la gestion sectorielle des identités au sein du système autrichien d'administration en ligne, ainsi que du contrôle de ce système de gestion.
Activités d'inspection	
Contrôles, enquêtes	16, la plupart en matière de vidéosurveillance.
Activités de sanction	
Sanctions	Néant. La DPA autrichienne ne peut imposer de sanctions.
Amendes	Néant. La DPA autrichienne ne peut infliger d'amendes.
DPD	
Chiffres relatifs aux DPD	Néant. Le droit autrichien ne prévoit pas de DPD.

B. Jurisprudence

1. Sécurité des données des compteurs de gaz

Pendant l'année de référence, la Commission de protection des données a adressé à un fournisseur de gaz une **recommandation** lui conseillant de prendre des mesures de sécurité des données pour ses **compteurs de gaz** en accès libre afin de **prévenir l'accès par des personnes non autorisées** aux données personnelles stockées dans les compteurs de gaz.

L'auteur de la réclamation s'était plaint que, dans le cadre de l'installation de nouvelles conduites de gaz dans le bâtiment protégé où il vit, les compteurs de gaz devaient être installés dans le couloir, de sorte que la consommation (le cas échéant) et les volumes consommés, etc. seraient accessibles à un nombre illimité d'inconnus (locataires et leurs familles, livreurs, etc.).

Le fournisseur de gaz a répondu que, concernant l'emplacement des compteurs, il convenait de tenir compte des lignes directrices de sécurité techniques (conditions générales du réseau de distributeurs de l'association autrichienne du gaz et de l'eau, ÖVGW), des exigences légales et des espaces disponibles à l'intérieur du bâtiment. Il n'y avait, par ailleurs selon lui, pas lieu de conclure à quelque « ingérence massive » dans les droits de protection de données de l'auteur de la réclamation, l'existence de données à caractère personnel était contestable, et la présence ou l'absence de la personne concernée dans l'appartement ne saurait être déduite d'une simple lecture du compteur.

La Commission de protection des données a conclu que des **mesures de garantie de la sécurité des données** devaient être prises pour l'ensemble des unités organisationnelles d'un client utilisant des données (à caractère personnel). Selon le type, le champ d'application et la finalité des données utilisées, et compte tenu, notamment, de l'état de la technologie et du caractère économique

raisonnable, il convient de s'assurer que les données ne sont pas accessibles à des personnes non autorisées.

Le fait que des personnes non autorisées (en conséquence d'une installation en un lieu généralement accessible, comme en l'espèce) **puissent avoir accès sans aucune restriction à des données à caractère personnel** couvertes par le droit fondamental à la protection des données (article 1er de la DSG 2000) constitue une violation de ce droit fondamental de la personne concernée (le consommateur).

2. Références personnelles dans le cadre de statistiques

Pendant l'année de référence, la Commission de protection des données a émis une **recommandation** à l'attention d'un fonds d'assurance maladie qui envoyait, sur simple demande, aux entreprises intéressées de plus de 50 salariés, des statistiques groupées sur les maladies des employés sur une année donnée en adaptant la structure des statistiques à chaque entreprise intéressée.

Les évaluations statistiques étaient structurées de manière à répertorier les différents groupes de maladies dans une colonne en regard de laquelle les chiffres relatifs aux maladies étaient répertoriés, dans d'autres colonnes, par sexe, par nombre total d'employés touchés, par nombre total de jours de congés maladie, une fois encore répertoriés par sexe, et par nombre de salariés concernés.

Ce transfert de statistiques groupées avait vocation à faciliter les mesures visant à promouvoir la santé au travail.

Le plaignant craignait que les données fournies ne soient pas indirectement personnelles ou anonymisées dans tous les cas et, par conséquent, qu'il soit possible pour une entreprise d'établir un lien direct entre un diagnostic et des employés.

La Commission de protection des données, partageant ces préoccupations, a conseillé au fonds d'assurance maladie de n'appliquer la distinction entre employés masculins et féminins (et la ventilation associée aux maladies typiques de ces groupes, telles que les maladies liées aux organes reproducteurs) qu'en cas de présence de plus de cinq personnes dans l'un de ces groupes. La Commission de protection des données estime que ce chiffre suffit à garantir l'impossibilité d'identifier des employés spécifiques.

Le fait qu'un employeur puisse identifier un employé en tirant des conclusions des statistiques groupées fournies constitue, en vertu de la section 1(1) de la DSG 2000, une violation du droit au secret de l'employé affecté pour ce qui concerne ses données à caractère personnel. Les données sur la santé étant des données sensibles au sens de la section 4 nº 2 de la DSG 2000, des normes particulièrement strictes doivent être appliquées.

La Commission de protection des données a également confirmé le principe énoncé par la Cour constitutionnelle selon lequel, même pour des statistiques essentiellement non personnelles, il convient de s'assurer que leur publication ne puisse permettre l'identification de données spécifiques (dignes de protection et de fait protégées par le droit fondamental à la protection des données) (cf. VfSlg 12.228/1989). Ce principe est également reflété par la section 46(1) de la DSG 2000, qui ne prévoit une utilisation privilégiée des données obtenues pour d'autres enquêtes ou à d'autres fins, que si l'investigation scientifique prévue ou les statistiques n'ont pas vocation à permettre de tirer des conclusions sur les personnes.

BELGIQUE

A. Résumé des activités et actualités

Modifications de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (loi «Vie privée»)

1. Suspension (sous conditions) du droit d'accès lors d'un contrôle ou d'une enquête fiscale par le ministère des Finances

L'article 3 de la loi «Vie privée» – qui, pour certains traitements de données identifiés, prévoit un régime dérogatoire – prévoyait depuis 2012, entre autres dérogations, une suspension du droit d'accès aux données relatives aux traitements gérés par le Service public fédéral (ministère des) Finances durant la période pendant laquelle la personne concernée est l'objet d'un contrôle, d'une enquête ou d'actes préparatoires à ceux-ci.

Cette mesure ayant été jugée inacceptable par la Commission de la protection de la vie privée notamment[5], une modification de cet article est intervenue en 2013. Il y est désormais prévu que le droit d'accès est certes suspendu pendant les circonstances précitées, *mais uniquement dans la mesure où la mise en œuvre de ce droit d'accès nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires* ***et*** *pour leur seule durée*. La durée de ces actes préparatoires pendant laquelle le droit d'accès n'est pas applicable *ne peut excéder un an à partir de la demande d'accès*.

L'exception est par ailleurs immédiatement levée après la clôture du contrôle ou de l'enquête, ou dès la clôture des actes préparatoires lorsque ceux-ci n'ont pas abouti à un contrôle ou une enquête. Le Service de sécurité de l'information et protection de la vie privée (organe de contrôle interne) créé au sein du Service public fédéral Finances en informe le contribuable concerné sans délai et lui communique dans son entièreté *la motivation* contenue dans la décision du responsable du traitement ayant fait usage de l'exception.

Pendant cette période de suspension du droit d'accès aux conditions ci-dessus, la personne concernée dispose d'un droit d'accès indirect – comme en matière policière – qu'elle exerce par l'intermédiaire de la Commission de la protection de la vie privée (article 13 de la loi «Vie privée»).

2. Création d'un organe de contrôle de la gestion de l'information policière au sein de l'autorité de protection des données (loi du 18 mars 2014)

La loi du 18 mars 2014 crée auprès de la Commission pour la protection de la vie privée un organe de contrôle de l'information policière chargé du contrôle du traitement des informations et des données visées par la loi relative à la fonction de police. Dans l'exercice de ses missions, cet organe est indépendant de la Commission de la protection de la vie privée, dont il partage toutefois le secrétariat. Essentiellement composé de membres des polices fédérale et locale ainsi que d'experts, l'organe doit compter un commissaire de l'autorité de contrôle (Commission de la protection de la vie privée) parmi ses membres.

L'organe de contrôle est particulièrement chargé de contrôler le respect des règles d'accès direct à la B.N.G. (banque nationale de données policières) et d'interrogation directe de celle-ci, ainsi que de contrôler le respect par l'ensemble des membres des services de police de l'obligation d'alimenter cette banque de données. Il veille, par le biais d'enquêtes de fonctionnement, à ce que le contenu de la B.N.G. et la procédure de traitement des données et informations qui y sont conservées soient conformes aux règles prescrites par la loi sur la fonction de police et à leurs mesures d'exécution, en particulier la régularité des opérations de traitement telles que la saisie des données et informations enregistrées en

[5] Commission de la protection de la vie privée, avis 32/2012 du 17 octobre 2012 (http://www.privacycommission.be). Dans un arrêt du 25 mars 2014, la Cour constitutionnelle de Belgique, saisie d'une demande d'annulation de la modification initiale (avant révision en 2013) annule cette disposition.

fonction du caractère concret ou de la fiabilité de celles-ci, ou encore l'effacement et l'archivage des données et informations à l'échéance de leurs délais de conservation. Les banques de données particulières (à durée limitée dans le temps par exemple) font également l'objet d'un contrôle. L'organe dispose de pouvoirs d'enquête et rapporte, ponctuellement et/ou annuellement, à la Chambre des représentants.

Vers une modification des articles 3 et 9 (droit à l'information) de la loi «Vie privée» ? Affaire Institut des professionnels de l'immobilier c. Englebert et autres portée devant la Cour constitutionnelle belge et la Cour de justice de l'Union européenne (CJUE)

L'affaire visait à savoir si la loi belge, en ne prévoyant pas d'exceptions pour les détectives privés comparables à celles visées à l'article 13, paragraphe 1, sous d) et g), de la directive 95/46, transpose correctement cette disposition. En effet, en ne prévoyant pas d'exception particulière pour les détectives privés, l'obligation d'information leur est applicable. La question se posait alors de savoir si, d'une part, il y avait une inégalité de traitement dans le chef des détectives privés et, d'autre part, si l'exercice de la profession de détective privé était encore possible dans ces conditions. En Belgique, la profession de détective privé est réglementée par une loi du 19.07.1991.

Saisi en 2012, le Tribunal du commerce a, au vu des questions qui se posaient, interrogé la Cour constitutionnelle belge. Cette dernière a, quant à elle, interrogé la CJUE.

La CJUE a rendu son arrêt le 7 novembre 2013 (C-473/12): http://curia.europa.eu/juris/document/document.jsf?text=&docid=144217&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=182002; la Cour constitutionnelle belge a rendu son arrêt le 3 avril 2014: http://www.const-court.be/public/f/2014/2014-059f.pdf

La Cour constitutionnelle belge a jugé que la disposition en cause de la loi «Vie privée» belge du 8 décembre 1992 viole les articles 10 (principe d'égalité) et 11 (principe de non-discrimination) de la Constitution belge dans la mesure où l'obligation d'information s'applique automatiquement à l'activité d'un détective privé ayant été autorisé à exercer ses activités pour des personnes de droit public conformément à l'article 13 de la loi du 19 juillet 1991 «organisant la profession de détective privé» et agissant pour un organisme professionnel de droit public (Institut des professionnels de l'immobilier) qui est chargé par la loi de rechercher des manquements à la déontologie d'une profession réglementée (agents immobiliers).

Modification de la loi relative aux communications électroniques – nouvelle compétence pour la Commission de la protection de la vie privée en matière de *data breach*

Depuis avril 2014, c'est la Commission de la protection de la vie privée, et non plus l'Institut belge des télécommunications, que les entreprises fournissant des services de communications électroniques accessibles au public doivent avertir en cas de violations de données. La Commission avertira elle-même l'Institut. La Commission est également tenue de veiller au respect par ces entreprises de la notification de la violation aux particuliers lorsque celle-ci s'impose. Un partenariat entre l'Institut belge des télécommunications et la Commission de la protection de la vie privée intervient par la suite.

Modification du paysage institutionnel de la protection des données

Aux côtés de la *Vlaamse toezichtcommissie* (commission de contrôle de l'échange des données entre administrations flamandes dans le cadre de l'administration électronique), une commission de contrôle des échanges de données aux niveaux régionaux wallon et bruxellois a été créée.

Activités de l'autorité de protection des données

Le rapport annuel de la Commission de la protection de la vie privée détaille l'ensemble de ses activités. Quelques-unes méritent une attention particulière (cf. http://www.privacycommission.be):

- Sensibilisation des mineurs : la Commission belge de la protection de la vie privée a initié la mise sur pied d'une pièce de théâtre comique et éducative sur le thème de la protection des données (activités en ligne et vie privée) s'adressant aux élèves de l'enseignement primaire (en néerlandais uniquement). Elle a élaboré un kit pédagogique complet, «Je suis jeune et je protège ma vie privée», dont un volet prend appui sur la pièce de théâtre précitée. Voir le site spécifique http://www.jeddecide.be et http://www.ikbeslis.be

- Violations de données – *data breach:* À la suite de plusieurs fuites importantes de données (dont la copie d'un fichier de la clientèle de la société de chemins de fer belge concernant 1,4 million de personnes), la Commission belge de la protection de la vie privée (CPVP) a élaboré un certain nombre de recommandations destinées à prévenir de telles fuites, le plus souvent dues à une sécurisation insuffisante des données traitées.

- Travaux sur le projet de règlement UE (*EU data protection reform*): la CPVP a rendu deux avis importants dans le contexte de la réforme de la protection des données négociée au sein de l'Union européenne. Son avis 35/2012 porte sur la proposition de règlement initialement déposée par la Commission européenne, et son avis 10/2014 porte sur le texte voté par la Commission LIBE en octobre 2013.

Organisation	Commission de la protection de la vie privée
Président et/ou collège	Du 1er janvier 2013 au 2 mai 2013 inclus Président: W. Debeuckelaere (magistrat) 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 2012 Du 2 mai 2013 au 31 décembre 2013 Président: W. Debeuckelaere (magistrat) Vice-président: S. Verschuere Collège effectif: A. Junion (avocate), F. Robben (administrateur général de la Banque-carrefour de la sécurité sociale et de la plate-forme e-health), J. Baret (secrétaire général honoraire du SPF Justice), E. Gheur (administrateur gérant de Galaxia et chargé de cours à l'université de Luxembourg), G. Vermeulen (professeur de droit à l'université de Gand), S. Waterbley (conseiller général à la DG Télécommunications et société de l'information du SP Économie) Collège suppléant: M. Salmon (conseillère Cour d'appel de Bruxelles), S. Mertens de Wilmars (enseignant), F. Schuermans (avocat général près la Cour d'appel de Gand), Y. Roger (président du Comité sectoriel de la sécurité sociale et de la santé) 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	6 840 000 euros
Personnel	53 employés (1 président – 1 vice-président) - Secrétariat de la présidence (5): secrétaires-juristes (2), secrétaires (2), logistique (1) - Administrateur (1) - Chefs de sections (3) - Personnel et organisation (16): comptable (1), traducteurs (5), secrétariat administratif (3), statistiques (1), responsable du personnel (1), accueil (2), logistique (1), support informatique (1), responsable de la communication (1) - Études et recherches (17): conseillers juridiques (15), spécialiste IT (1), documentaliste (1) - Relations extérieures (*Front Office*) (11): conseillers juridiques (4), assistants (7)
Activités générales	
Décisions, avis, recommandations	Avis (à la demande du pouvoir législatif ou exécutif – voir plus bas): 69 - Avis et recommandations d'initiative: 5 - Recommandations dans le cadre des déclarations de traitements ultérieurs: 11
Notifications	6 047 dossiers de déclarations en 2013 et un total de 5 252 nouveaux traitements déclarés. 436 déclarations de modifications/corrections à des traitements de données existants et 359 déclarations de fin de traitement
Contrôles préalables	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 se sont vu adresser le nombre de demandes d'autorisations suivant: - Comité sectoriel Autorité fédérale: 44 autorisations individuelles - Comité sectoriel statistiques: 28 autorisations individuelles - Comité sectoriel du Registre national: 87 autorisations individuelles - Comité sectoriel de la sécurité sociale et de la santé: voir le site de la Banque-carrefour de la sécurité sociale https://www.ksz-bcss.fgov.be/fr/bcss/nodepage/content/websites/belgium/security/committee_03.html
Demandes émanant de personnes	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	concernées ou de responsables de traitement: La CPVP a traité 3 532 demandes d'information ou de médiation (y compris des dossiers de contrôle). Ces dossiers peuvent être répartis comme suit: 2 871 demandes d'informations émanant tant d'instances publiques et de responsables de traitement actuels ou futurs que de personnes concernées, 450 demandes de médiation et 211 dossiers de contrôle. Son «Front Office» a en outre traité 2 868 dossiers répartis sur les thèmes suivants: utilisation de caméras de surveillance (14,85 %), principes de protection des données (8,12 %), travail (5,47 %), économie (3,35 %) (questions sur le crédit à la consommation) et autorités publiques (2,24 %).
Plaintes émanant de personnes concernées	La CPVP a reçu 450 plaintes, soit une hausse de 48,5 % par rapport au nombre de plaintes reçues en 2012 (303). Ces plaintes concernent principalement les domaines suivants: - Principes de protection de la vie privée (27,6 %): principe de proportionnalité, non-respect du principe de finalité, du devoir d'information - Enregistrement de mauvais payeurs auprès de la Centrale des crédits aux particuliers de la Banque nationale de Belgique (13,6 %) - Vidéosurveillance (12,4 %) - Marketing direct (5,1 %) - Internet (4 %)
Conseils sollicités par le Parlement ou le gouvernement	La liste des avis émis par la Commission belge en 2013 est disponible sur son site internet à l'adresse: http://www.privacycommission.be
Autres renseignements relatifs aux activités générales	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	211 dossiers de contrôles. En 2013, la Commission de la protection de la vie privée a effectué des contrôles à deux niveaux. Le premier niveau est celui des traitements effectués dans le cadre, d'une part, des systèmes d'information Schengen, Eurodac et Douane et, d'autre part, des activités d'Europol. Le deuxième niveau concerne les contrôles effectués d'initiative. Ces contrôles peuvent être subdivisés en trois types: les contrôles permanents auprès de Child Focus et du Centre d'information et d'avis sur les organisations sectaires nuisibles; les contrôles thématiques auprès des services de police et de renseignements, dont font partie les dossiers relatifs à l'accès indirect (relevant de l'article 13 de la loi «Vie privée» – secteur police); et des contrôles ponctuels qui visent toujours un responsable de traitement spécifique.
Activités de	

sanction	
Sanctions	La CPVP ne dispose pas de compétence de sanction propre. Elle peut toutefois transmettre au parquet les dossiers dans lesquels elle constate des infractions.
Amendes	La CPVP ne dispose pas de compétence de sanction propre. Elle peut toutefois transmettre au parquet les dossiers dans lesquels elle constate des infractions.
DPD	
Chiffres relatifs aux DPD	La CPVP ne dispose pas de cette information.

BULGARIE

A. Résumé des activités et actualités

Organisation	
Président et/ou collège	En vertu de l'article 7 (1) de la loi sur la protection des données à caractère personnel (LPDP), la Commission de protection des données à caractère personnel (CPDP) est une autorité collective composée d'un président et de 4 membres. En 2013, la structure de la CPDP était la suivante : Mme Veneta Shopova, présidente, et 4 membres : M. Krassimir Dimitrov, M. Valentin Enev, Mme Mariya Mateva et M. Veselin Tselkov.
Budget	2 700 000 BGN, dont 2 693 530 BGN dépensés.
Personnel	Nombre de fonctionnaires employés : 67
Activités générales	
Décisions, avis, recommandations	En 2013 : 357 décisions, avis et instructions ont été émis au total, dont : - 252 plaintes - 79 avis sur l'application de la LPDP - 26 instructions contraignantes
Notifications	42 308 responsables du traitement des données à caractère personnel
Contrôles préalables	2 613 contrôles préalables
Demandes émanant de personnes concernées	123 demandes émanant de personnes physiques et morales, et diverses demandes sur des thèmes d'actualité liés aux compétences de la CPDP.
Plaintes émanant de personnes concernées	450 plaintes — la plupart émanant des secteurs suivants : - Télécommunications : 333 - Services d'assurance et du travail : 42 - Banques et services bancaires : 33 - Santé et éducation : 13 - Autres : 29
Conseils sollicités par le Parlement ou le gouvernement	Pendant la période considérée, le Conseil des ministres a envoyé les 2 demandes d'avis suivantes :

	- Demande d'avis concernant deux demandes d'accès à des informations publiques : un organe de presse a demandé une liste des employés au sein du Conseil de l'administration ministérielle, contenant les noms, les postes et les rémunérations prévues par les contrats. - Demande d'avis concernant une question posée par deux députés via le président de l'Assemblée nationale au Premier ministre de la République de Bulgarie en vertu de l'article 90 (1) de la Constitution de la République de Bulgarie et de l'article 89 des règles d'organisation et de procédure de l'Assemblée nationale. Les informations demandées portaient sur le nombre de fonctionnaires employés et licenciés au sein de l'administration publique sur une période de 6 mois, spécifié par l'organisme de la manière suivante : Ministères, agences publiques, agences exécutives, administrations locales et administrations spécialisées – personnes morales.
Autres renseignements relatifs aux activités générales	13 notifications et 12 demandes d'approbation de transferts de données vers des pays tiers ont été reçues. Pour la première fois, une demande basée sur les règles d'entreprise contraignantes a été déposée. Cet instrument n'étant pas prévu par la législation bulgare, la Commission a dans ce cas approuvé le transfert au motif de l'article 36b de la LPDP, à savoir, sur la base des preuves fournies quant aux obligations contractuelles entre le responsable du traitement et le destinataire, qui apportaient des garanties suffisantes pour leur protection. Concernant la procédure établie par le groupe de travail « Article 29 » sur les règles d'entreprise contraignantes (BCR), la CPDP a approuvé 15 BCR d'autorités chefs de file et accepté les décisions de l'autorité chef de file dans le cas de 5 BCR.
Activités d'inspection	
Contrôles, enquêtes	En 2013, 2 696 contrôles ont été menés au total : - ex ante 2 613 ; - en cours 39 ; - ex post : 44, la plupart dans les secteurs suivants : santé : 1 510 ; commerce et services : 310 ; éducation et formation : 225 ; services juridiques et autres prestations de conseil : 136 ; construction et architecture : 62 ; tourisme : 51.
Activités de sanction	
Sanctions	En 2013, dans le cadre de ses activités administratives et pénales, la CPDP a prononcé et imposé :

	- 30 conclusions de violations administratives - 29 amendes
Amendes	En 2013, la CPDP a imposé des amendes et des sanctions matérielles pour un montant de 76 800 BGN
DPD	
Chiffres relatifs aux DPD	S. o. La LPDP ne prévoit pas la désignation de délégués à la protection des données.

B. Informations sur la jurisprudence

1. Concernant les instructions contraignantes formulées et les amendes imposées

En 2013, 26 instructions contraignantes ont été prononcées, dont la plupart dans le secteur de l'administration publique, suivi par ceux des administrations locales et municipales, des finances, des assurances et de la santé. Des instructions contraignantes ont été formulées dans les secteurs suivants : justice, éducation et formation, technologies de l'information, commerce et services.

Les instructions ont été formulées en lien avec :

- l'absence des mesures organisationnelles et techniques nécessaires pour garantir le niveau de protection des données à caractère personnel : 44 % des décisions ;
- l'incapacité à prendre les mesures nécessaires pour mettre à jour les informations des registres des responsables du traitement de données : 18 % ;
- le traitement illicite de données à caractère personnel : 25 % ;
- le traitement de données à caractère personnel sans le consentement informé de la personne concernée : 13 %.

En 2013, la CPDP a imposé 29 amendes. Aucune n'a été annulée par le tribunal, et une a été confirmée avec une réduction du montant de l'amende. De toutes les amendes imposées en 2011 et 2012 ayant fait l'objet d'un appel et d'une décision du tribunal en 2013, 3 ont été intégralement annulées, 12 ont été confirmées, dont 6 avec une réduction du montant. À l'heure actuelle, 25 amendes sont en attente d'un jugement. En 2013, cinq amendes ont été appliquées sans faire l'objet d'un appel.

Parmi les violations les plus courantes de la CPDP figuraient les suivantes :

- violation des principes de licéité, de proportionnalité des données à caractère personnel traitées, et de traitement à des finalités déterminées, explicites et légitimes : 15 violations ;
- traitement sans exigence légale d'admissibilité du traitement : 20 violations pour lesquelles des sanctions matérielles ont été imposées ;
- incapacité à prendre les mesures techniques et organisationnelles nécessaires pour protéger les données contre leur destruction accidentelle ou illicite ou contre leur perte accidentelle et contre tout accès non autorisé, toute rectification ou diffusion et autres formes illégales de traitement : 19 violations pour lesquelles des sanctions matérielles ont été imposées ;
- traitement avant que le responsable du traitement ait déposé une demande d'inscription au registre des responsables du traitement et des registres qu'il administre et qui sont tenus à jour

par la Commission : 3 violations pour lesquelles des sanctions matérielles et des amendes ont été imposées ;

- traitement à des fins de marketing direct sans laisser à la personne la possibilité de refuser le traitement : 5 violations pour lesquelles des sanctions matérielles ont été imposées ;
- refus d'aider la Commission dans l'exercice de ses pouvoirs de supervision : 4 violations pour lesquelles des sanctions matérielles ont été imposées ;
- incapacité à prendre une décision sur les demandes d'accès à des données à caractère personnel : 2 violations ;
- absence de notification au registre de vidéosurveillance : 4 violations.

2. Concernant la formulation d'avis sur des demandes et signalements

En dehors des demandes adressées à la CPDP par les autorités publiques visées au tableau ci-dessus, les avis suivants sont intéressants :

2.1. Avis de la CPDP sur des demandes d'accès à la base de données démographiques nationale

En 2013, diverses demandes ont également été formulées concernant l'accès à la base de données démographiques nationale tenue à jour par la direction générale des services d'état civil et administratifs (DG CRAS) au ministère du développement régional et des travaux publics, ou aux registres d'état civil.

Les responsables du traitement de données à caractère personnel ont continué à demander à bénéficier d'un accès direct à la base de données démographiques nationale, motivés par la présence d'un intérêt juridique ou par leurs activités et l'exercice des obligations qui leur sont imposées par le droit (par exemple, les établissements de crédit demandent à bénéficier d'un accès dans le cadre des exigences d'identification de leurs clients découlant des dispositions de la loi sur les mesures anti-blanchiment).

La pratique de la CPDP vis-à-vis des demandes d'accès direct à la base de données démographiques nationale consiste à distinguer la communication d'informations (données) de la base de données en vertu d'un intérêt juridique prouvé et l'octroi d'un accès direct à la base de données.

La Commission a formulé un avis selon lequel il n'existait aucun obstacle juridique à ce que la DG CRAS du ministère du développement régional et des travaux publics communiquent des informations particulières, c'est-à-dire des données à caractère personnel (sans accès direct) aux parties qui en font la demande si celles-ci apportent la preuve de leur intérêt légal en vertu des procédures établies.

2.2. Demandes d'accès à des informations publiques

La législation bulgare en matière de protection des données ne réglemente pas les questions liées à la liberté d'information et à l'accès aux informations, qui sont prévues par d'autres lois.

Malgré cela, en 2013, la CPDP s'est également prononcée sur des demandes d'avis d'autorités publiques et locales en lien avec les demandes d'accès à des informations publiques.

2.2.1. Demandes adressées aux autorités publiques concernées (Conseil des ministres) pour la communication d'informations sur :

- les noms, les postes et la rémunération de personnes sous contrats de travail et officiels, ainsi que les copies de contrats. Dans ce cas, la CPDP est d'avis que les informations demandées

dans un tel volume appartiennent à la catégorie des « données à caractère personnel » dans la mesure où elles permettent l'identification des personnes et que leur traitement n'est admissible qu'avec le consentement des personnes concernées.

- le nombre de fonctionnaires employés et licenciés au sein de l'administration publique sur une période de 6 mois, selon le statut de l'organisme : ministères, agences publiques, agences exécutives, administrations locales et administrations spécialisées. Il a été demandé au Conseil des ministres de communiquer une liste avec des noms et des informations sur les motifs d'emploi. Il a également été souligné que la communication de ces informations permettrait d'identifier les structures administratives particulières. Dans ce cas, les informations ont pu être fournies (sans les noms des personnes) afin de respecter l'obligation juridique du responsable du traitement.

2.2.2. Autres demandes d'accès à des informations

L'adjoint à l'office des forêts du ministère de l'agriculture et des forêts a demandé la communication d'informations contenant des données à caractère personnel sur des fichiers liés au changement d'utilisation et à la vente de parcelles de forêts. Avant que les informations demandées ne soient fournies, il convient de tenir compte des exigences juridiques et de l'intérêt du public quant aux questions soulevées par les membres du Parlement, et aussi en ce qui concerne le droit à la vie privée et l'existence du consentement des personnes concernées. La CPDP a estimé que le responsable du traitement des données à caractère personnel pouvait communiquer les fichiers contenant des informations sur les ventes et changements d'utilisation prévus pour les parcelles après que les données à caractère personnel qu'ils contiennent avaient été modifiées afin de ne plus permettre l'identification des personnes, en effaçant les noms ou en les anonymisant par le biais de leurs initiales.

2.3. Concernant les demandes liées à la prévention des conflits d'intérêts par l'occupation de postes de haut niveau au sein de l'administration publique

En 2013, la CPDP a dû gérer un autre problème important lié à l'accès aux informations contenant des données à caractère personnel : l'annonce des déclarations relevant de la loi sur la prévention et la divulgation de conflits d'intérêts sur les sites Web officiels des institutions publiques. Cherchant à équilibrer l'intérêt public et la protection des données à caractère personnel de personnes en particulier, la Commission a accepté que la publication de déclarations devrait avoir lieu après l'obtention du consentement explicite écrit des personnes affectées dans le cadre d'un texte distinct de ces mêmes déclarations. La publication sur Internet de déclarations relevant de la loi sur la prévention et la divulgation de conflits d'intérêts sans le consentement explicite des personnes serait une violation de la LPDP. Aussi, toute déclaration publiée sur des sites officiels sans consentement devrait être retirée jusqu'à ce qu'un consentement explicite ait été obtenu. L'annonce ne doit pas contenir la signature du déclarant. Lorsque la déclaration contient des données à caractère personnel d'autres personnes, le consentement de la personne affectée n'a pas à être demandé et ses données devraient être anonymisées.

2.4. Concernant l'accès à des données sensibles contenues dans des registres spéciaux

Les autres avis de la CPDP en 2013 ont porté sur des problèmes liés à l'accès à des données dites « sensibles » dont le traitement est généralement interdit en vertu de l'article 5 (1) de la LPDP.

Prenons à titre d'exemple le cas d'un hôpital psychiatrique public de Bulgarie approché par la direction régionale du ministère de l'intérieur lui demandant de fournir une « liste à jour des personnes souffrant de maladies mentales actuellement hospitalisées ». Dans ce cas, la CPDP a émis un avis selon lequel l'exigence relative à la tenue d'une liste de personnes souffrant de maladies mentales par des inspecteurs de police visée à l'article 20 (1) (7) de l'instruction 13-2295 de 2012, dans le cadre de

l'organisation des opérations du ministère de l'intérieur sur les services territoriaux aux citoyens, est contraire aux conditions applicables à la communication d'informations en vertu de l'article 28 (1) de la loi sur la santé, qui protège les droits des patients et, dans ce cas particulier, les droits des patients souffrant de maladies mentales hospitalisés au sein de l'établissement psychiatrique public en question.

La Constitution de la République de Bulgarie contient par ailleurs plusieurs principes de base concernant les personnes souffrant de maladies mentales, à savoir que les personnes atteints de troubles physiques et mentaux bénéficient de la protection spéciale de l'État et de la société (article 51 (3)) et que l'État doit protéger la santé de ses citoyens (article 52 (3)). Le texte de l'instruction est en outre en conflit absolu avec les dispositions de l'article 157 (1) de la loi sur le ministère de l'intérieur, qui interdit explicitement la collecte d'informations sur le seul état de santé des citoyens. Au vu de ce qui précède, la Commission a exprimé un avis selon lequel les informations demandées (liste à jour des personnes souffrant de maladies mentales hospitalisées sous traitement) ne devaient pas être fournies. La communication de ces informations serait contraire aux dispositions de l'article 4 (1) et de l'article 5 (2) de la LPDP, de l'article 28 de la loi sur la santé et de l'article 157 (1) de la loi sur le ministère de l'intérieur.

Dans ce cas, fournir les informations demandées sur les personnes traitées au sein de cet hôpital serait une violation des principes de limitation de la finalité et de proportionnalité visés à l'article 2 (2) de la LPDP.

2.5. Avis concernant les élections des membres du Parlement

En 2013, la CPDP a exprimé un avis sur demande du président et du secrétaire de la Commission électorale centrale, concernant l'élection des membres du Parlement.

Tout d'abord, la question de la nécessité de l'inscription à la CPDP a été soulevée au sujet des comités d'initiatives pour la nomination de candidats indépendants à l'Assemblée nationale. La Commission a déclaré que les comités d'initiatives pour la nomination de candidats indépendants en vertu de l'article 96 (2) du Code électoral sont des responsables du traitement de données à caractère personnel tenus de s'inscrire à la CPDP.

La deuxième question portait sur l'élection des membres du Parlement, ainsi que sur les amendements et suppléments au Code électoral adoptés en février 2013 et imposant de nouvelles obligations à la Commission électorale centrale (CEC). En lien avec l'une de celles-ci, portant sur la diffusion des réunions de la CEC en direct sur Internet, la CPDP a exprimé un avis selon lequel cette pratique était licite et admissible, en considérant que l'obligation établie légalement découlait des dispositions du nouveau Code électoral et de l'exécution des tâches relevant de l'intérêt public, comme assurer la possibilité pour le public d'être informé sur les sujets importants évoqués dans les réunions de la CEC.

2.6. Avis de la CPDP sur la mise en œuvre en Bulgarie de la loi relative au respect des obligations fiscales concernant les comptes étrangers de contribuables américains

La Commission a exprimé un avis sur une question de grand intérêt d'un point de vue financier : la mise en œuvre en Bulgarie de la loi relative au respect des obligations fiscales concernant les comptes étrangers de contribuables américains (FATCA), adoptée par le Congrès américain.

La demande a été déposée par les représentants d'une banque sise en Bulgarie et faisant partie d'une multinationale. La loi FATCA a pour principal objectif de permettre aux autorités fiscales des États-Unis de combattre les fraudes transfrontalières commises par des américains ayant des comptes et des actifs financiers à l'étranger. Cet objectif sera atteint en déployant un système mondial d'échange automatique d'informations imposant à l'ensemble des établissements financiers étrangers de fournir

des informations aux autorités fiscales américaines (Internal Revenue Service – IRS) sur tous les comptes de contribuables américains ou de sociétés étrangères détenues par des contribuables américains. Aussi la loi FATCA crée-t-elle de nombreuses nouvelles obligations pour l'ensemble des établissements financiers étrangers. Après une analyse approfondie, la CPDP a présumé que, puisque la banque bulgare n'était, à l'heure actuelle, aucunement tenue de fournir les données à caractère personnel de ses clients (les personnes relevant de la loi fiscale américaine) à un autre responsable du traitement de données aux États-Unis dans le cadre de la mise en œuvre de la loi FATCA, il n'existait aucune base juridique pour que la CPDP permette le transfert de ces données vers les États-Unis. Le transfert de données reposant uniquement sur le consentement des personnes serait excessif et contraire au principe de légalité du traitement de données à caractère personnel en raison de l'absence de base réglementaire pour demander le consentement des personnes.

C. Autres informations importantes

Pendant la période considérée, la Commission de protection des données à caractère personnel a adopté une nouvelle ordonnance sur le niveau minimal de mesures techniques et organisationnelles, et le type admissible de protection des données à caractère personnel

Le 30 janvier 2013, la Commission de protection des données à caractère personnel a adopté une nouvelle ordonnance concernant le niveau minimal de mesures techniques et organisationnelles, et le type admissible de protection des données à caractère personnel. L'ordonnance a été émise au motif de l'article 23, paragraphe 5, de la loi sur la protection des données à caractère personnel. Elle a été publiée au Journal officiel le 12 février 2013. Cette ordonnance abroge l'ordonnance nº1 du 7 février 2007.

Cette ordonnance vise à assurer une protection des données à caractère personnel adéquate suivant la nature des données et le nombre de personnes concernées en cas de violation. Les principales finalités de la protection des données à caractère personnel sont définies comme étant la confidentialité, l'intégrité et la disponibilité. Cinq niveaux de protection des données à caractère personnel sont introduits : protection physique, protection personnelle, protection documentaire, protection des réseaux et/ou systèmes d'information automatisés, et protection cryptographique. L'ordonnance introduit par ailleurs le principe du « besoin d'en connaître ».

Afin de déterminer le niveau adéquat de mesures techniques et organisationnelles et le type de protection admissible, les responsables du traitement sont tenus d'évaluer régulièrement les impacts sur les données à caractère personnel traitées.

L'évaluation de l'impact vise à définir les niveaux d'impact et de protection appropriés. Les mesures techniques et organisationnelles que doivent prendre les responsables du traitement de données à caractère personnel sont déterminées pour chaque niveau de protection.

Les nouvelles règles prévoient quatre niveaux d'impact suivant l'importance des conséquences négatives pour les personnes à la suite du traitement non autorisé de données à caractère personnel : « extrêmement élevé », « élevé », « moyen » et « faible ».

Depuis l'entrée en vigueur de l'ordonnance, la Commission de protection des données à caractère personnel a ouvert des consultations et a commencé à former des responsables du traitement de données à caractère personnel afin de les sensibiliser aux nouvelles règles de protection.

L'ordonnance (https://www.cpdp.bg/en/index.php?p=element&aid=632) est disponible en anglais sur le site Internet de la CPDP.

La Commission de protection des données à caractère personnel se concentre sur la formation des responsables du traitement de données à caractère personnel conformément au plan de formation annuel adopté. Les experts de la CPDP interviennent, en tant que conférenciers, sur des questions liées à la protection des données à caractère personnel dans les cours de l'institut de l'administration publique, le seul centre de formation national des fonctionnaires.

CHYPRE

A. Résumé des activités et actualités

Le bureau du commissaire a été consulté sur un certain nombre de propositions législatives européennes, telles que, notamment, le paquet de propositions pour la protection des données présenté par la Commission en janvier 2012, et les propositions régulant Europol et Eurojust, dans le cadre de questions liées à la protection des données à caractère personnel.

Le bureau du commissaire a activement participé aux travaux du Conseil de l'Europe pour la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, en prenant part aux comités T-PD et CAHDATA du Conseil de l'Europe.

Dans le cadre des activités de célébration de la journée européenne de la protection des données, le bureau du commissaire a alloué un budget de 4 300 € pour la diffusion, le 28 janvier, de documents informatifs imprimés et de cadeaux (réveils et lampes torches) portant le logo et l'adresse électronique du bureau. Le message de cette journée était : *il est temps de se réveiller et de comprendre*. Le commissaire et ses délégués ont fait plusieurs apparitions à la télévision et à la radio.

Suite à l'examen d'une plainte déposée par des employés par le biais de leurs syndicats contre un hôpital privé qui avait installé un système de contrôle de présence des employés utilisant des données biométriques (empreintes digitales) stockées sur des cartes à puces remises aux employés et non stockées dans une base de données centrale, une décision a été publiée, concluant que l'utilisation de ce type de système était en violation du principe de proportionnalité. L'hôpital a été appelé à cesser le traitement des données et à désinstaller le système. L'hôpital n'a pas respecté la décision et l'a contestée devant le tribunal. Le jugement est en attente.

Organisation	Bureau du commissaire à la protection des données à caractère personnel
Président et/ou collège	M. Yiannos Danielides
Budget	Budget alloué : 257 352 € Budget exécuté : 225 120 €
Personnel	Agents administratifs : 7 Agents informaticiens : 2 Secrétaires : 6 Agents auxiliaires : 2
Activités générales	
Décisions, avis, recommandations	Avis : 61 Décisions : 5 Recommandations : 2
Notifications	278
Contrôles préalables	S. o.
Demandes émanant de personnes concernées	Par écrit ou par téléphone : S. o.
Plaintes émanant de personnes concernées	Spams : 308 Autres : 77

Conseils sollicités par le Parlement ou le gouvernement	En 21 occasions, notre bureau a été invité à des réunions des comités parlementaires de la Chambre des représentants pour des conseils/consultations
Autres renseignements relatifs aux activités générales	Autorisations de regroupement de fichiers : 16 Autorisations de transmission vers des pays tiers : 50
Activités d'inspection	
Contrôles, enquêtes	Nombre d'audits : 1
Activités de sanction	
Sanctions	Dans 3 décisions sur 5, des sanctions administratives ont été imposées. Dans les 2 autres décisions, le commissaire a adressé des recommandations aux responsables du traitement.
Amendes	Dans 2 des 3 décisions où des sanctions administratives ont été imposées, les responsables du traitement ont respectivement reçu des amendes de 3 000 € et 300 €.
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

En 2012, le bureau du commissaire a examiné une plainte contre une société d'assurance accusée d'avoir demandé à la plaignante un nombre disproportionné de documents médicaux afin d'appuyer sa demande d'indemnisation pour incapacité de travail en raison de son état de santé. Ayant examiné les conditions du contrat d'assurance et le nombre de documents (supplémentaires) parfois exigés de la plaignante, le commissaire a, en 2013, publié une décision concluant que l'incapacité de la compagnie d'assurance à accepter ou rejeter la demande d'indemnisation dans un délai raisonnable, compte tenu du nombre proportionnel de documents parfois exigés de la plaignante et du prolongement de l'examen en demandant des tests et documents supplémentaires, constituait une violation du principe de proportionnalité et a imposé une sanction administrative de 3 000 €à la compagnie d'assurance. La décision du commissaire a été contestée devant le tribunal et le jugement est en attente.

C. Autres informations importantes

La décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, a été transposée dans la législation nationale le 20 décembre 2013 en vertu d'une décision du conseil des ministres. Le droit national désigne le commissaire comme étant l'autorité de contrôle compétente stipulée par la décision.

CROATIE

A. Résumé des activités et actualités

Organisation	
Président et/ou collège	Anto Rajkovača
Budget	5 482 847 HRK (1 € = 7,5 HRK)
Personnel	28
Activités générales	
Décisions, avis, recommandations	1 091
Notifications	21 978 (1 648 en 2013)
Contrôles préalables	
Demandes émanant de personnes concernées	Les demandes ne sont pas enregistrées de manière distincte
Plaintes émanant de personnes concernées	212
Conseils sollicités par le Parlement ou le gouvernement	17
Autres renseignements relatifs aux activités générales	L'agence a adopté une nouvelle structure organisationnelle privilégiant le renforcement des activités d'inspection.
Activités d'inspection	
Contrôles, enquêtes	330
Activités de sanction	
Sanctions	87
Amendes	2
DPD	
Chiffres relatifs aux DPD	2 037 DPD enregistrés (643 en 2013)

Pendant la période considérée, la DPA croate a consacré l'essentiel de son temps aux campagnes visant à sensibiliser l'opinion publique à l'importance de la protection des données à caractère personnel. Nous vous informerons par conséquent des activités les plus importantes déployées sur cette période :

- L'introduction publique de l'application en ligne « Bouton rouge » du ministère de l'intérieur, destinée à rapporter les abus ou l'exploitation sexuels des enfants en coopération avec le partenariat pour l'établissement d'un « centre pour un Internet plus sûr » fonctionnel (dont l'agence croate de protection des données à caractère personnel est l'un des partenaires stratégiques), le tout dans l'objectif de sensibiliser le public à une utilisation sûre d'Internet et de promouvoir une utilisation sûre, responsable, adéquate et efficace d'Internet par les enfants et les jeunes ;

- Lors de la journée de la protection des données 2013, l'agence a organisé une conférence de presse de gala et différentes activités telles que la désignation de nouveaux ambassadeurs du respect de la vie privée (des personnalités qui, en dépit de leur popularité, bénéficient d'une réputation positive) dont la mission consiste à promouvoir le respect de la vie privée et la protection des données à caractère personnel ;

- À l'occasion de son 10e anniversaire, en mai 2013, l'agence a organisé les différentes activités suivantes, qui ont reçu un très bon accueil de la part du public croate :

  1) **Conférence de presse de gala « 10 mesures contre les discours de haine sur Internet »** qui s'est tenue au Parlement croate en présence de nombreuses personnalités de la vie politique et culturelle croate, telles que les ambassadeurs du respect de la vie privée, qui ont lu les témoignages dramatiques de deux adolescents croates gravement traumatisés après avoir subi de très sévères formes de cyberharcèlement lors de cette période délicate qu'est l'adolescence. Cette lecture a permis d'adresser au public un message très important sur les conséquences des discours de haine. Un rapport détaillé de cette conférence a été diffusé aux heures de grande écoute par NOVA TV dans le cadre de son principal programme d'information, qui bénéficie en Croatie des taux d'audience les plus élevés. Des représentants du ministère de l'intérieur, du réseau de recherche universitaire (CARNET) et de l'association des journalistes croates ont également présenté leurs points de vue sur la question.

  2) L'agence est très fière de produire de la **documentation promotionnelle** délivrant des messages éducatifs sur le sujet des discours de haine sur Internet :

     - affiche éducative « 10 mesures contre les discours de haine sur Internet » ;

     - affiche en rouleau 1 : « Surfons sur des vagues positives ! » ;

     - affiche en rouleau 2 : « Nous sommes tous responsables ! ».

  3) **La Conférence des délégués à la protection des données et des délégués à l'information,** avec 5 imminents conférenciers (experts) venus proposer des présentations très intéressantes sur les dernières tendances en matière de protection des données et autres domaines associés. L'agence a été vivement remerciée pour avoir eu l'initiative d'organiser cette conférence, source d'informations des plus utiles pour plus de 100 participants.

DANEMARK

A. Résumé des activités et actualités

Organisation	
Président et/ou collège	La gestion des affaires courantes 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	Env. 22,5 millions de DKK
Personnel	Env. 35
Activités générales	
Décisions, avis, recommandations	S. o. (inclus dans les chiffres ci-dessous)
Notifications	2 777
Contrôles préalables	2 777
Demandes émanant de personnes concernées	2 221 Ce nombre couvre l'ensemble des demandes et plaintes déposées devant la DPA danoise
Plaintes émanant de personnes concernées	Voir ci-dessus
Conseils sollicités par le Parlement ou le gouvernement	468
Autres renseignements relatifs aux activités générales	14 affaires liées à la sécurité
Activités d'inspection	
Contrôles, enquêtes	45
Activités de sanction	
Sanctions	Chaque année, la DPA danoise adresse ses critiques à plusieurs responsables du traitement des données pour leur non-respect de la loi sur le traitement des données à caractère personnel
Amendes	S. o.
DPD	
Chiffres relatifs aux DPD	S. o. (ceci n'est pas une option en vertu de la législation danoise)

B. Informations sur la jurisprudence

Établissements publics utilisant des réseaux sociaux

En octobre 2013, l'Agence pour la protection des données (DPA) danoise a reçu une demande d'un établissement public concernant son utilisation des réseaux sociaux et, plus particulièrement, de Twitter et Facebook. L'établissement avait prévu un projet pilote dans le cadre duquel il serait plus présent publiquement sur les réseaux sociaux.

Dans cette situation, la DPA danoise a principalement soulevé deux points. Tout d'abord, l'autorité devrait gérer ses publications sur les réseaux sociaux de manière à exclure toutes données à caractère personnel. Les personnes physiques sont, en règle générale, responsables du traitement des données de leurs propres publications sur les réseaux sociaux.

Ensuite, s'il sera possible pour les citoyens de contacter les autorités via les systèmes de messagerie interne des réseaux sociaux, alors ces autorités pourront devenir responsables du traitement de ces données, comme il est possible de considérer les réseaux sociaux comme des sous-traitants. C'est pourquoi les autorités doivent tenir compte de la gestion du système de messagerie interne.

Si les autorités sont considérées comme des responsables du traitement de données et les réseaux sociaux comme des sous-traitants, alors lesdites autorités seront responsables de la sécurité des données et pourront avoir à conclure un accord de traitement avec les réseaux sociaux, tout en prenant en compte la réglementation relative au transfert de données vers des pays tiers.

Les données à caractère personnel lors de la scission d'une entreprise

En mars 2013, la DPA danoise a reçu une demande d'un cabinet d'avocats concernant une société destinée à être scindée en plusieurs sociétés indépendantes lors d'une restructuration. La question se posait, notamment, de savoir si la société serait considérée comme étant en situation de succession, ou si l'on devait considérer les données à caractère personnel des clients comme étant transférées vers une autre société.

La DPA danoise a conclu qu'en règle générale, cette situation serait considérée comme un transfert de données, dans la mesure où celles-ci passeraient d'une société à une autre. Dans certains cas, toutefois, il sera possible de considérer la situation comme correspondant à une succession de société.

Dans ce type de situation, les éléments suivants doivent être respectés : La relation avec les clients (droits et obligations) est transférée, les actifs transférés resteront fonctionnels, la division consécutive de la société doit être strictement définie, la société est autonome et le seul objet du transfert est la restructuration.

Si la situation ci-dessus est observée, elle peut être considérée comme une succession au regard des données à caractère personnel. Il revient au responsable du traitement de données de procéder à l'analyse préliminaire.

C. Autres informations importantes

Vidéosurveillance dans les taxis

Depuis 2010, les taxis danois doivent légalement s'équiper de systèmes de vidéosurveillance. La DPA danoise a par conséquent réalisé une série d'enquêtes auprès des sociétés de taxis afin de confirmer que ces installations de vidéosurveillance respectaient la réglementation sur la protection des données, et de recueillir des informations sur la manière dont les responsables du traitement de données géraient la vidéosurveillance.

La DPA a observé que, dans l'ensemble, les sociétés de taxis avaient suffisamment compris les exigences en matière de protection des données, et n'a rien découvert de flagrant lors de ses enquêtes.

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 grand public sur la protection des données par le biais d'un événement en interne. Le personnel a organisé des visites des bureaux, donné des présentations et tenu une séance de questions-réponses pour les participants. La journée a été un succès pour le personnel comme pour les visiteurs qui ont fait preuve de connaissances approfondies et d'un grand intérêt pour la protection des données à caractère personnel.

ESPAGNE

A. Résumé des activités et actualités

Après la hausse constante de ces dernières années, l'activité de l'agence en 2013 est restée aux niveaux atteints en 2012, notamment en ce qui concerne les activités liées aux plaintes et aux contrôles. Bien que les chiffres affichent une légère réduction, ils restent élevés avec 10 600 plaintes déposées par des citoyens et plus de 10 700 décisions finales émises par l'agence.

Tout au long de l'année 2013, nous avons continué de travailler à l'élaboration de mesures visant à promouvoir les connaissances, et à faciliter l'exercice des droits des citoyens et la conformité réglementaire. En ce sens, l'agence a lancé une nouvelle chaîne thématique sur son site web appelée « Protégez vos informations en ligne », ainsi qu'une série de vidéos d'instructions où est démontrée, étape par étape, la manière de configurer les options de son navigateur et des réseaux sociaux, ainsi que le fonctionnement général du système en matière de vie privée. D'autres documents seront publiés sur cette chaîne dans le futur. L'élargissement des services offerts via notre plateforme de services en ligne, lancée en 2012, mérite une mention particulière, ainsi que l'optimisation de tous les services d'information fournis via notre site web, tels que l'actualisation de certaines des lignes directrices les plus populaires à l'attention des responsables du traitement de différents secteurs.

Concernant les activités de contrôle et l'exercice des pouvoirs de sanction, il convient de souligner que, malgré la stabilité des chiffres sur les résolutions punitives, on peut observer une augmentation considérable du pourcentage de décisions (84 % du total) où l'amende a été réduite par l'application des nouveaux critères introduits par une loi passée en 2011 pour réduire la sévérité des sanctions en tenant compte d'éléments tels que le comportement du responsable du traitement, l'existence de mesures de responsabilisation ou les conséquences réelles de l'infraction. D'un autre côté, nous avons pu observer une légère baisse du nombre de décisions où les sanctions économiques ont été remplacées par des « avertissements préventifs », qui représentent 24 % de l'ensemble des décisions de sanction.

L'agence maintient également ses efforts visant à assurer une meilleure protection des enfants. À cet égard, elle a lancé en octobre 2013 son nouveau site éducatif, qui vise à fournir aux enfants et aux éducateurs des informations et des outils intéressants. Ce site web réunit l'ensemble des documents éducatifs précédemment publiés par l'agence et inclut de nouveaux outils spécifiquement développés pour ce site.

Organisation	Agence espagnole de protection des données
Président et/ou collège	José Luis Rodríguez Álvarez
Budget	13 524 070 €
Personnel	158
Activités générales	
Décisions, avis, recommandations	
Notifications	602 531
Contrôles préalables	S. o.
Demandes émanant de personnes concernées	102 064

Plaintes émanant de personnes concernées	10 604
Conseils sollicités par le Parlement ou le gouvernement	318
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	2 299
Activités de sanction	
Sanctions	874
Amendes	22 339 440
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

En 2013, l'Audiencia Nacional (cour d'appel des décisions de l'agence) a émis 274 résolutions, dont :

-188 rejetant l'appel contre les décisions de l'agence (68 %)

-33 acceptant en partie la demande de l'appelant (12 %)

-53 acceptant totalement la demande (20 %)

La Cour suprême a émis 12 sentences dans des cas de recours contre les jugements de l'Audiencia Nacional. Dans tous les cas, le sens de la sentence a confirmé la position de l'agence.

L'Audiencia Nacional a également décidé de s'adresser à la Cour de justice de l'UE pour un jugement préliminaire dans une affaire de « droit à l'oubli ». Cette affaire est l'une des près de deux cents affaires en attente de jugement et relève de la plainte déposée par un citoyen devant l'agence contre Google. L'agence a émis une décision demandant à Google de supprimer un certain nombre de résultats de recherche. Google a fait appel de cette décision.

Les deux principaux problèmes de cette demande de décision préjudicielle sont les suivants :

a. D'une part, l'applicabilité de la directive 95/46 vis-à-vis des services offerts par Google Inc. aux citoyens européens. Dans ce but, la Cour a posé une série de questions liées à l'applicabilité de l'article 4.1 de la directive, dans la mesure où Google Spain, SL, une filiale de Google Inc., déploie des activités avec le moteur de recherche et où Google Spain, SL a été expressément désignée par Google Inc. comme étant son représentant aux fins du transfert à cette dernière des plaintes et demandes légales émanant de citoyens espagnols. La Cour a également demandé que soit clarifiée la notion de « moyens situés sur le territoire d'un État membre ». En ce sens, la Cour a directement mentionné l'article 8 de la CEDH, déclarant qu'il serait juste d'appliquer la loi du pays où a lieu le conflit afin d'assurer efficacement la protection des citoyens.

b. D'autre part, une série de questions a été posée sur la nature même des moteurs de recherche. Tout d'abord, et compte tenu de la définition du traitement des données énoncée par la directive, la Cour a posé la question de la possibilité de considérer l'indexation comme traitement de données à caractère personnel au sens de la directive 95/46. Sous réserve que la réponse soit positive, la seconde question portait sur la nature réelle des responsabilités légales de l'entité offrant le service, qu'elles soient directes ou complètes ou que celle-ci soit simplement une filiale du responsable du traitement chargé du site web où les informations ont été traitées à l'origine. Compte tenu de ce qui précède, et conformément aux critères de la CJCE, il serait possible de faire une interprétation en s'adressant directement au responsable du traitement du moteur de recherche afin d'éviter l'indexation des informations affectées.

C. Autres informations importantes

En 2013, l'agence pour la protection des données de la communauté autonome de Madrid a cessé ses activités. Ses compétences ont été récupérées par l'État et assumées par la DPA espagnole.

Concernant l'étendue des activités de l'agence, la modification de la loi réglementant le pouvoir judiciaire (loi organique nº 4/2013) modifie les pouvoirs de son instance dirigeante (conseil général du pouvoir judiciaire), y compris celui de « collaboration avec l'autorité de contrôle de la protection des données dans le domaine de l'administration de la justice. L'agence assumera par ailleurs les compétences de cette autorité uniquement en ce qui concerne les activités des juges et des magistrats en lien avec l'utilisation de dossiers judiciaires ».

Dans un autre registre, l'agence a conclu en 2013 une procédure de sanction contre Google liée à la nouvelle politique de l'entreprise en matière de respect de la vie privée. Cette procédure a été ouverte en juin 2013 dans le cadre de la mise en application coordonnée convenue par le groupe de travail et dirigée par la CNIL (France). La décision finale a déclaré l'existence de trois violations graves de la loi organique sur la protection des données à caractère personnel (LOPD), a imposé à Google une amende de 300 000 euros pour chacune, et a demandé que l'entreprise mette en œuvre sans délai les mesures nécessaires pour respecter les exigences juridiques applicables. Les trois infractions relèvent de la collecte et du traitement illicites d'informations personnelles d'utilisateurs authentifiés ou non et d'utilisateurs passifs ; du stockage et de la conservation de données sur des périodes indéterminées ou injustifiées ; et l'absence de mécanismes permettant l'exercice des droits d'accès, de rectification, d'annulation et d'opposition.

ESTONIE

A : Résumé des activités et actualités

Les technologies de l'information et des communications et la société de l'information se développent rapidement. C'est pourquoi la zone « grise » qui entoure l'acquisition de modes de protection des données à caractère personnel et d'informations publiques est de plus en plus vaste.

Des concepts juridiques non définis (dommages excessifs et intérêt public, par exemple) requièrent par conséquent d'être constamment interprétés. Compte tenu de la modestie de l'espace juridique et linguistique estonien, nos pratiques spécialisées dans les domaines de la justice et de la terminologie juridique prennent plus de temps à se développer que dans les plus grands pays.

L'autorité de contrôle estonienne doit par conséquent se focaliser sur la création de lignes directrices et le développement de pratiques juridiques pour assurer la clarté et la certitude juridiques essentielles dans le cadre des affaires et de l'administration publique.

Chaque année, l'autorité de contrôle estonienne traite un sujet important de ladite zone « grise », organise une forme de surveillance, des enquêtes et des discussions avec les parties concernées, et s'inspire des idées professionnelles et des problèmes pratiques.

*

L'an dernier, le sujet central était l'emploi de matériel de surveillance et d'enregistrement. Nous avons essayé d'aborder ce sujet de manière complexe : utilisation de caméras à des fins privées, enregistrement dans un lieu public et dans le cadre d'un événement public, caméras de sécurité, enregistrement destiné à s'assurer de l'application d'un contrat et à des fins journalistiques, caméras dans les établissements pour enfants, éducatifs et publics, etc. L'une des questions sources de débats a, par exemple, été de savoir si les jardins d'enfants et les établissements scolaires étaient des lieux publics du point de vue des enregistrements et de la prise de photos (où le consentement n'est pas nécessaire) et, si oui, dans quelle mesure.

La conseillère juridique de l'autorité de contrôle estonienne, Maris Juha, a initié la préparation de « lignes directrices sur l'utilisation de caméras », nos premières directives publiées dans le système d'information du projet législatif.
*

Outre la préparation de nouvelles lignes directrices, nous essayons également de maintenir « en vie » nos autres lignes directrices importantes, de nous y référer dans le cadre de notre travail quotidien et de prévoir les changements nécessaires. Outre la directive sur le traitement des données à caractère personnel dans les relations d'emploi, préparée en 2011, il s'est avéré nécessaire de mieux couvrir le respect de la vie privée des employés utilisant des ordinateurs et des dispositifs intelligents.

Tandis que les relations personnelles sont couvertes par la confidentialité des messages et les obligations de protection des données et de garantie du secret des entreprises de communication, l'utilisation des mêmes dispositifs dans les relations d'emploi crée un triangle juridique : l'employé n'est pas le client de l'entreprise de communications. La directive « Caractère privé de l'utilisation d'un ordinateur par un employé », initiée par le conseiller informatique de l'autorité de contrôle estonienne Urmo Parm, associe technologies de l'information et explications juridiques.

Outre la publication de réponses aux questions les plus intéressantes pour les employés et les employeurs dans la FAQ de notre site Web, nous les publierons également sur le portail consacré à la vie professionnelle géré par l'inspection du travail.

*

L'an dernier, plusieurs problèmes ont été observés dans le domaine des assurances : l'utilisation de données de tiers, le stockage des consentements au traitement de données à caractère personnel et les mouvements des données des clients d'un courtier changeant d'employeur. À l'initiative de l'inspecteur en chef Merit Valgjärv, nous avons également contrôlé des sociétés de leasing dans le cadre de la transmission de données à caractère personnel aux compagnies d'assurance.

Dans le domaine bancaire, nous avons procédé à des examens du traitement de données à caractère personnel sur la base de contrats et de consentements, et organisé un contrôle destiné à avoir un aperçu des pratiques. Les principaux problèmes observés avaient un lien avec les consentements au marketing direct. Les banques ont depuis ajusté leurs pratiques en la matière.

Sur la base des problèmes observés dans la pratique, nous avons apporté des améliorations importantes à la directive sur la publication des défauts de paiement.

*

La création du groupe informatique de l'autorité de contrôle a grandement amélioré les activités d'explication et de sensibilisation dans le domaine des technologies de l'information et de communications. Nous publierons des instructions et des explications pratiques dans la presse et sur le Web. Les neuf recommandations pratiques pour l'utilisation sûre d'un smartphone de notre conseiller informatique Urmo Parm comptabilisent plus de 21 000 vues sur le mur Facebook de l'autorité de contrôle. Les instructions concernant les applications Facebook ont été vues plus de 10 000 fois. Les instructions concernant la configuration du navigateur de l'ordinateur d'un enfant (à l'attention des parents) ont été vues près de 10 000 fois, et les lignes directrices relatives à la suppression de l'historique de l'utilisateur d'une carte d'identité sur un ordinateur ont été vues 4 000 fois.

Nous avons également déployé des activités de sensibilisation à travers plusieurs formes de coopération : dans le cadre du projet Targalt Internetis (Soyez intelligents en ligne !), avec l'association des enseignants d'histoire et d'études sociales, et des gardiens du Web. À l'initiative du conseiller Silver Sarapuu, nous avons préparé des bandes dessinées sur la protection de la vie privée destinées à servir de documents d'aide aux enseignants dans les établissements scolaires.

*

En coopération avec l'université de Tartu, nous avons organisé la conférence « Dimensions éthiques de la protection des données et de la vie privée : enjeux mondiaux et locaux », les 9 et 10 janvier 2013. L'impressionnante sélection des intervenants a permis d'écouter plusieurs éminents scientifiques estoniens et conférenciers reconnus à l'international, tels que le professeur Beate Rössler et le Contrôleur européen de la protection des données Peter Hustinx. Le parrain de la conférence était le président de la République, qui a également assuré la première présentation sur le sujet. Une conférence concernant des activités de sensibilisation et d'explication du secteur financier a été organisée en coopération avec le centre d'éthique de l'université de Tartu.

Pour un événement de recherche de si haut niveau et, en même temps, si exhaustif, nous devons tout d'abord remercier le responsable du centre d'éthique de l'université de Tartu, le professeur Margit Sutrop, et son équipe. Les participants à cette conférence étaient essentiellement des spécialistes du domaine juridique ou des technologies de l'information, et je pense que tous ont été impressionnés par la conceptualisation de leur travail quotidien via des valeurs éthiques.

*

L'approbation des bases de données du système de gestion des informations de l'État est une procédure inter-agences qui peut sembler difficile et ennuyeuse vue de l'extérieur et pour laquelle le public ne montre que peu d'intérêt. La procédure d'approbation du système d'information sur les ventes de tickets des transports publics de Tallinn s'est avérée être une exception.

Les autorités locales ayant ignoré les remarques juridiques et relatives à la sécurité des informations de l'autorité de contrôle et de l'autorité publique du système d'information, et utilisé une base de données non coordonnée, nous avons ouvert des procédures de supervision distinctes, auxquelles nous avons fait participer des experts de ladite autorité et du centre des registres et des systèmes d'information. Les périodes de stockage des données personnalisées ont par conséquent été réduites, la sécurité a été renforcée, la législation locale a été modifiée, et la base de données a été soumise à des procédures de concertation.

Tous les changements apportés suite à cette supervision devraient avoir lieu en temps voulu pendant l'approbation du plan d'établissement de la base de données ou l'approbation de la mise en œuvre au plus tard.

Nous pensons qu'il peut s'agir, pour toutes les agences publiques nationales et locales, d'un exemple édifiant : résoudre rétrospectivement les problèmes de protection des données dans les bases de données est plus coûteux et plus contraignant que de les éliminer en cours d'approbation.

Nous avons compilé des « lignes directrices sur les bases de données » visant à résoudre les problèmes pratiques liés à la régulation et à la gestion des bases de données.

*

Dans le cadre d'activités transfrontalières, nous avons poursuivi la coopération entre les inspections de protection des données des pays baltes et la supervision de sujets convenus fondée sur une méthodologie commune.

Nous avons complété le contrôle tripartite des hôtels de la marque Radisson Blue Hotel. Lors du contrôle de casinos, nous avons découvert une faille dans la législation estonienne quant à la période de stockage maximale d'enregistrements vidéo et d'information de clients. Pour la corriger, nous avons émis une recommandation en coopération avec les services répressifs et le syndicat des organisateurs de jeux de hasard.

Les agences pour la protection des données du Global Privacy Enforcement Network (GPEN, ou réseau mondial d'application des lois pour la protection de la vie privée) ont supervisé l'opération « Internet Sweep Day » en mai 2013. Dans ce cadre, nous avons examiné l'existence et l'exhaustivité des politiques de confidentialité de 40 des plus grandes entreprises de vente au détail d'Estonie.

D'après la directive, l'activité du groupe de travail des autorités européennes de protection des données, formé sur la base de l'article 29 de la directive 95/46/CE, consiste à améliorer la mise en œuvre harmonisée de la directive. À ce jour, l'activité la plus prenante du groupe de travail a été la préparation d'avis (lignes directrices), un domaine où nous avons acquis des compétences considérables. Les conseils stratégiques sont également traités, comme récemment avec la réforme des droits européens de protection des données afin de coordonner la résolution d'affaires qui avaient attiré l'attention de la communauté internationale et, si nécessaire, une autorité membre obtient le droit d'agir au nom de tout le groupe de travail.

En octobre 2013, l'autorité de contrôle a présenté une initiative à la séance plénière du groupe de travail afin d'inscrire régulièrement à l'ordre du jour l'organisation d'une coopération pratique : un échange d'expériences managériales et un accord sur une plus grande fluidité des procédures de coopération transfrontalière. Des collègues du Royaume-Uni se sont joints à cette initiative et y ont apporté leur soutien. Dans chacune des séances plénières suivantes, tous les points du programme conjointement préparés ont été discutés.

*

Dans sa réponse aux violations, la priorité de l'autorité de contrôle est toujours de mettre le plus rapidement possible un terme à la violation plutôt que de la sanctionner.

Cette approche est également préconisée par le rapport « Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE », publié par l'Agence des droits fondamentaux de l'Union européenne en janvier 2014. En effet, les personnes dont les droits ont été violés sont principalement intéressées par la cessation rapide de cette violation.

D'après l'autorité de contrôle, les litiges liés à la disponibilité des informations publiques répondent au même objectif : les personnes qui déposent des demandes souhaitent bénéficier de procédures rapides et faciles pour accéder aux informations.

En comparaison, dans les cas de supervision liés à la protection des données à caractère personnel et des informations publiques, 287 propositions-recommandations et seulement 53 principes ont été publiés. Dans la plupart des cas, la violation prend fin à réception d'une proposition ou d'une recommandation.

Le nombre de mesures punitives (procédures contraventionnelles) a diminué et celles-ci portent principalement sur des abus de droits d'accès professionnels à des dossiers sensibles. La violation ayant déjà eu lieu, la supervision par voie de propositions-principes n'a plus de raison d'être, et c'est la raison pour laquelle l'autorité de contrôle répond toujours en initiant des procédures contraventionnelles dans ces cas.

La situation du registre de la population s'est sensiblement améliorée. Nous reconnaissons des années de contrôles systématiques par le ministère de l'intérieur responsable du registre. Les interventions de l'autorité de contrôle dans les médias à ce sujet ont probablement été utiles.

Au cours de l'audit sur la protection des données de l'administration routière, nous avons examiné la vulnérabilité des données à caractère personnel de la partie non divulguée du registre de la circulation, qui inclut les coordonnées des personnes sur la base du registre de la population. L'administration routière a aujourd'hui mis en œuvre des mesures technique et de contrôle interne afin de prévenir tout abus et, sur la base d'un accord conclu l'an dernier, notifie l'autorité de contrôle de ses soupçons de violation en vue d'ouvrir une procédure contraventionnelle.

Organisation	Autorité de contrôle de la protection des données estonienne
Président et/ou collège	Directeur général
Budget	631 329 €
Personnel	18
Activités générales	
Décisions, avis, recommandations	601
Notifications	602 enregistrements de traitements de données sensibles à caractère personnel
Contrôles préalables	15
Demandes émanant de personnes concernées	1 370
Plaintes émanant de personnes concernées	550

Conseils sollicités par le Parlement ou le gouvernement	52
Autres renseignements relatifs aux activités générales : approbation de bases de données du secteur public (y compris refus)	89
Activités d'inspection	
Contrôles, enquêtes	463
Activités de sanction	
Sanctions	22 cas
Amendes	3 206 €
DPD	
Chiffres relatifs aux DPD	121

FINLANDE

A. Résumé des activités et actualités

Dans le cadre de la mise en œuvre de la stratégie du bureau du médiateur chargé de la protection des données au cours de l'année considérée, nous avons restructuré notre système de gestion du personnel et mieux intégré notre programme de gestion des compétences internes au système. Afin de prolonger notre réussite dans un environnement opérationnel volatil, nous devons garantir la qualité et la quantité de compétences internes. Les autres pierres angulaires de notre stratégie comprennent la capacité à prédire l'impact de nouveaux phénomènes et à classer nos mesures par ordre de priorité, l'utilisation des informations en tant qu'outil de pilotage, et la formation des alliances nécessaires tout en conservant notre indépendance et notre impartialité.

Le bureau a également réussi à obtenir le niveau requis par le décret gouvernemental sur la sécurité des informations. Dans le cadre de ces efforts, l'ensemble du personnel a dû passer un test sur la sécurité des informations. La formation à la sécurité des informations est un élément permanent de notre programme de gestion des compétences.

Nous avons pris des mesures pour lancer un service entièrement nouveau, le service d'informations, et pour restructurer notre personnel. Le développement de la gestion interne des informations fait partie de cette approche. Je pense que la plus grande part des problèmes qui nous ont été signalés a déjà été commentée ou a fait l'objet d'une réaction de notre part. Nous devons nous concentrer sur des problèmes essentiels pour assurer la gestion efficace des ressources et le maintien continu du niveau de service.

Indépendamment de l'exécution du règlement ou de la directive sur la protection des données, nous avons conscience du besoin pressant, au regard des compétences dans notre pays, de pourvoir au nombre croissant de postes de délégués à la vie privée disponibles. C'est pourquoi nous avons lancé un sondage interne afin d'enquêter sur la possibilité de créer un label de qualité certifiant la formation. Cet effort de développement de produit doit être déployé en coopération avec les organismes éducatifs conformément à notre stratégie.

Dans le cadre de nos efforts en faveur d'une efficacité maximale, nous avons poursuivi nos enquêtes sur le secteur commercial et spécifiques aux phénomènes. Ces enquêtes ont, entre autres, porté sur les services téléphoniques financés par la publicité, le secteur des prêts sur salaire, l'utilisation commerciale des données à caractère personnel, et la sécurité des informations des sites Web étudiée grâce la coopération internationale (Sweep Day).

Des mécanismes de cohérence et une coopération internationale ont été déployés en collaboration avec nos collègues norvégiens à l'occasion du lancement d'un audit conjoint d'un conglomérat international de services de musique en ligne. L'audit a été terminé en cours d'année.

La protection des données des entrepreneurs faisait partie des sujets que nous avons étudiés en priorité. Les entrepreneurs ont été ciblés par différentes opérations de ventes forcées. Afin d'assurer leur protection sur le plan juridique, il est important de respecter l'équilibre des informations entre les parties en litige. Dans notre sphère de compétences, nous avons soutenu la fédération des entreprises finlandaises dans la résolution de ce problème.

Les biobanques ont été introduites parmi les groupes cibles des activités de protection des données à caractère personnel du médiateur chargé de la protection des données. L'autorité nationale de contrôle du bien-être et de la santé (Valvira) sera la principale autorité de contrôle.

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 1 708 000 EUR.
Personnel	L'effectif total comprend 20 personnes.
Activités générales	
Décisions, avis, recommandations	3 157
Notifications	535
Contrôles préalables	Voir notifications
Demandes émanant de personnes concernées	958
Plaintes émanant de personnes concernées	(Accès et rectifications) 269
Conseils sollicités par le Parlement ou le gouvernement	127
Autres renseignements relatifs aux activités générales	Collaboration avec des responsables du traitement des données dans les secteurs suivants : éducation, soins de santé, affaires sociales, télécommunications, emploi et économie, marketing
Activités d'inspection	
Contrôles, enquêtes	119
Activités de sanction	233
Sanctions	S. o.
Amendes	S. o.
DPD	
Chiffres relatifs aux DPD	> 1 000

B. Informations sur la jurisprudence

Affaires policières

Il est désormais de notoriété publique que des données à caractère personnel du président de la Russie ont été enregistrées dans le système d'information de la police finlandaise. Dans le même temps, des enquêtes étaient en cours quant à la consultation non autorisée des données d'un médaillé d'or olympique décédé. Au terme de l'enquête, des dizaines de fonctionnaires de police ont été reconnus

coupables d'une violation des dispositions de la législation sur les données à caractère personnel. La situation a menacé d'affecter la confiance du public en la police et la position des commandants de la police finlandaise. Selon moi, la chaîne de commandement des chefs de la police aux agents chargés du traitement des informations est trop longue et requiert l'inclusion d'activités de supervision plus proches des opérations.

Sécurité alimentaire

Les systèmes de fidélisation des consommateurs recueillent généralement des informations sur les habitudes de consommation avec l'autorisation des consommateurs. Aucune information spécifique aux produits n'est recueillie. L'autorité finlandaise de sécurité alimentaire Evira a été informée de la possibilité qu'un produit vendu par une chaîne de magasins ayant un système de fidélisation des consommateurs, contenait un produit toxique, le datura stramonium, obligeant des consommateurs à se rendre à l'hôpital pour suivre un traitement médical. En vertu de l'article 19 de la réglementation européenne générale en matière d'alimentation (règlement (CE), n° 178/2002 du Parlement européen et du Conseil), Evira a demandé au détaillant de prendre des mesures afin de connecter les informations de son système de fidélisation aux données relatives aux achats des magasins afin d'avertir les consommateurs qui avaient acheté le produit en question. Le détaillant s'est avéré en mesure de connecter ces données. S'en sont suivies d'intenses discussions concernant la crédibilité des systèmes de fidélisation et, d'un autre côté, la relation entre la protection des données et la sécurité des produits.

Marketing d'affiliation

La loi sur la protection de la vie privée dans les communications électroniques stipule qu'un consentement préalable est requis pour le marketing électronique direct qui cible des consommateurs. Le marketing d'affiliation a été créé de manière à contourner cette règle non équivoque. En marketing d'affiliation, la mesure marketing est prise par une société qui opère dans un pays où il est possible de refuser cette pratique, par exemple. La société qui souhaite vendre ses produits loue les services marketing de l'autre société tout en déclarant ne pas acquérir de services de traitement de données à caractère personnel ni de contenus de données à caractère personnel. Dans un type de marketing d'affiliation, l'espace de publication est acquis au sein de documents de communication marketing d'une autre société ou autres documents de communication. Le médiateur chargé de la protection des données est intervenu dans ces opérations. Les codes de conduite concernant ces actions marketing sont désormais préparés avec le secteur du marketing direct.

Définition d'un responsable du traitement de données à caractère personnel

J'ai appris que des représentants d'un groupe religieux s'étaient rendus chez des particuliers et avaient collecté des données à caractère personnel, en négligeant de respecter les obligations visées par la loi sur les données à caractère personnel. Le problème n'était pas de savoir si l'organisation avait le droit de collecter des données dans le cadre de ses activités, mais qui était responsable de ces opérations de collecte en tant que responsable du traitement. L'organisation a rejeté toute responsabilité et expliqué que le cas concernait l'utilisation de données à caractère personnel à des fins domestiques auxquelles la loi sur les données à caractère personnel ne s'appliquait pas. J'étais d'un avis différent et le comité de la protection des données, qui a agi en sa capacité d'autorité compétente en la matière, a déclaré partager mon point de vue. L'organisation a fait appel de la décision auprès d'un tribunal administratif.

C. Autres informations importantes

Le nouvel écosystème des communications mobiles pose un problème accru pour la protection des données, ainsi que la position et les droits des consommateurs sur un plan plus général. Les smartphones nous ont fait entrer dans l'ère des applications, ou applis. Le traitement de données à caractère personnel évolue, de registres de fichiers centraux traditionnels vers des systèmes de plus en

plus compliqués où un grand nombre d'applications est géré par des systèmes d'exploitation de dispositifs connectés à une infrastructure en réseau.

Dans ce contexte, une stratégie nationale de cyber-sécurité a été publiée en Finlande.

Le ministère des transports et des communications a réalisé une enquête sur le thème des mégadonnées, et le ministère des finances a désigné un groupe de travail pour mettre en œuvre un programme de données ouvertes. Les opérateurs ont continué de souffrir du manque de transfert d'informations entre les différentes autorités. Pour éliminer cette partie du problème due à l'absence d'une architecture de système d'information globale, il a été décidé qu'une nouvelle autorité qui emploierait plus d'un millier de personnes (Valtori) serait établie à des fins correctives. De la même manière, le canal des services aux citoyens a été développé, en partie sur la base de l'expérience estonienne.

Le cadre législatif concernant la protection des données à caractère personnel n'a cessé de se développer. D'un autre côté, le processus a accru nos obligations de contrôle. L'adéquation ou, plutôt, la rareté de nos ressources semble être une condition permanente selon l'étude réalisée en lien avec le projet NETSO et en attente de publication.

Le projet législatif de code de la société de l'information dirigé par le ministère des transports et des communications s'est déroulé sans heurts. Le projet a également soulevé la question de la neutralité d'Internet, ou de savoir si les communications sur Internet devaient rester libres ou si les opérateurs, par exemple, avaient le droit de traiter en priorité certains messages, à savoir ceux qui sont payés plus cher.

Le rapport du professeur Ahti Saarenpää a évoqué, conformément à ses paramètres, la nécessité potentielle d'un fichier de crédit positif. Le rapporteur a conclu qu'il vaudrait mieux observer en premier lieu l'impact du règlement européen sur la protection des données sur le traitement des informations financières. D'un autre côté, le rapporteur a proposé que les fichiers de crédit soient tenus d'être identifiés comme faisant partie des fichiers de données fondamentaux de la société, ce qui a donné lieu à l'attribution de privilèges légaux spéciaux.

Le travail du groupe de travail sur la taxation de la circulation routière présidé par M. Ollila a également suscité l'émotion.J'étais opposé au suivi en temps réel des conducteurs et ai proposé que, lorsque des données devaient servir de base à ladite taxation, elles devraient être collectées de manière distribuée.

Une étude que nous avons réalisée a montré que presque tous les opérateurs de télécommunications qui offrent des abonnements mobiles aux consommateurs proposent également une option de financement partiel via la publicité. Le consommateur doit consentir à recevoir des publicités en échange d'une réduction sur le prix de ses appels. D'après les autorités de protection des consommateurs, un téléphone est une nécessité. La directive sur la protection des données définit le consentement comme étant un acte légal unilatéral qu'il est possible de retirer. Les consommateurs s'abonnent fréquemment à un service partiellement financé par la réception de publicités, avant de retirer immédiatement leur consentement. Le médiateur chargé de la protection des données a établi que, dans le cas de ce type de produits nécessaires, le consentement ne pouvait faire partie du contrat client, mais devait plutôt être considéré comme une déclaration d'intention distincte. Les opérateurs ont par conséquent développé un système de double tarification spécial.

La communication au public des informations nécessaires constitue l'un des plus grands défis pour la protection des données. Afin de relayer des informations correctes et à jour, notre site Web était en cours de restructuration en 2013. Nous avons également participé au développement du concept global du magazine Tietosuoja et pris la décision d'établir un groupe de services d'information.

FRANCE

A. Résumé des activités et actualités

L'année 2013 a, encore une fois, montré une activité en forte croissance, démontrant la place prépondérante des données personnelles à l'ère numérique et une sensibilité croissante des citoyens à ce sujet. Face à cette activité en pleine expansion, la CNIL a poursuivi une action efficace et a accéléré sa mutation pour gagner encore en réactivité.

Le développement des outils de conformité

Tout au long de l'année 2013, la CNIL a poursuivi sa démarche d'accompagnement des professionnels en leur proposant de nombreux outils d'aide à la conformité, tels que : les correspondants « informatique et libertés », les labels, les règles internes d'entreprises (BCR) et la création de packs de conformité sectoriels.

Les correspondants « informatique et libertés » (CIL), acteurs de la co-régulation

Chaque année, le CIL s'affirme un peu plus comme un acteur central de la mise en conformité.

Fin 2013, 13 000 organismes avaient désigné un CIL, contre 11 000 un an plus tôt. La plus-value de la désignation d'un CIL s'apprécie particulièrement à l'occasion d'un nouveau projet impliquant un traitement de données personnelles grâce à ses conseils, lors de l'instruction d'une plainte ou d'un contrôle de la CNIL, ou enfin dans la facilitation de l'exercice des droits d'accès ou d'opposition.

Appelé à prendre la suite du CIL avec des missions renforcées, le futur délégué à la protection des données sera au cœur du modèle proposé par le projet de règlement européen.

Le label: un gage de confiance

La loi «informatique et libertés» permet à la CNIL de délivrer des labels «à des produits ou des procédures». Pour les entreprises, le label CNIL permet de se distinguer par la qualité de leur service. Pour les utilisateurs, c'est un indicateur de confiance dans les produits ou procédures labellisés, en leur permettant aisément d'identifier et de privilégier ceux qui garantissent un haut niveau de protection de leurs données personnelles.

Trois référentiels ont été créés à la demande d'organisations professionnelles: le label «formations» et le label «audit de traitement», adoptés en 2012, ainsi que le premier label produit, adopté en 2014, pour les services de coffre-fort numérique. Depuis 2012, ce sont 29 labels qui ont été délivrés par la CNIL.

Les packs de conformité

Suite à une large concertation avec les professionnels concernés, différents packs sectoriels ont été élaborés: le pack «assurance», le pack «logement social», le pack «compteurs communicants» et le pack «collectivités locales».

Les recommandations

La CNIL a élaboré plusieurs recommandations au cours de l'année 2013, permettant de préciser aux professionnels les conditions de mise en œuvre pratiques de la loi «informatique et libertés». Ces recommandations ont porté respectivement sur les cookies et autres traceurs, la conservation des données de cartes bancaires par les commerçants et les coffres-forts numériques.

Le conseil aux pouvoirs publics

En 2013, la CNIL a rendu 74 avis sur des projets de décrets ou de lois, dont:

- le projet de loi relative à la consommation, avec des dispositions prévoyant la mise en place d'un registre national des crédits aux particuliers;
- la transparence des liens d'intérêts dans le secteur de la santé;
- la transparence de la vie politique;
- la PNIJ (Plateforme nationale des interceptions judiciaires): texte réglementaire pas encore publié;
- le projet de loi relatif à l'utilisation de la géolocalisation dans le cadre des enquêtes judiciaires;
- le TAJ (Traitement des antécédents judiciaires);
- les téléservices publics locaux.

Par ailleurs, la CNIL met à disposition des parlementaires son expertise juridique et technologique et propose des actions d'information et de sensibilisation.

L'accompagnement de l'innovation

Dans le cadre de son activité d'innovation et de prospective, la CNIL renforce sa capacité d'écoute et de dialogue avec de très nombreux acteurs d'horizons divers. Cette démarche lui permet de mieux anticiper les évolutions technologiques et d'accompagner les nouveaux usages le plus en amont possible pour garantir une innovation durable, respectueuse des droits des utilisateurs.

La CNIL s'est ainsi dotée d'un laboratoire d'innovation en 2011, qui permet de tester des produits et applications innovants, de développer des outils mis à disposition du public tels que l'outil Cookieviz, qui a été téléchargé 62 500 fois, et de mener à bien des projets de recherche et développement comme le projet Mobilitics, en partenariat avec Inria.

Le suivi de la notification des violations de sécurité

Suite à l'entrée en vigueur du Règlement européen concernant les mesures relatives à la notification des violations de données à caractère personnel, en août 2013, la CNIL a mis en place une téléprocédure, accessible à partir de son site, pour permettre aux opérateurs de procéder aux notifications de façon sécurisée.

Faciliter l'exercice des droits

Les plaintes

En 2013, la CNIL a enregistré environ 5 640 plaintes, correspondant à une stabilisation des demandes. Ceci s'explique essentiellement par une meilleure orientation des demandes dès leur réception et par une mise en avant de contenus pratiques précisant davantage les cas dans lesquels la CNIL peut intervenir (ex.: les fiches pratiques sur les données personnelles au travail et sur la vidéosurveillance/vidéoprotection)

L'opposition à figurer dans un fichier, tous secteurs confondus, constitue le principal motif de plaintes, ainsi que l'exercice du droit d'accès. L'année 2013 a parallèlement confirmé la tendance observée

depuis 2011 quant au nombre important de plaintes relatives au secteur «internet/télécom» (34 % des plaintes reçues) et plus particulièrement aux problématiques d'e-réputation.

La CNIL a ainsi reçu 1 917 plaintes qui portent sur la suppression de textes, photographies, vidéos, coordonnées, commentaires, faux profils en ligne, la réutilisation de données publiquement accessibles sur internet, etc.

Le droit d'accès indirect

La CNIL a reçu 4 305 demandes de droit d'accès indirect, soit une augmentation de 17 % par rapport à 2012. Ces demandes représentent un total de 7 148 vérifications à mener concernant, par ordre d'importance, le fichier FICOBA de l'administration fiscale, les fichiers d'antécédents judiciaires de la police et de la gendarmerie (fichier unique TAJ depuis le 1er janvier 2014) et les fichiers de renseignement.

Sanctionner

Le 10 juin 2013, la présidente de la CNIL a adopté une mise en demeure à l'encontre de la société Google Inc. Le bureau de la CNIL (la présidente et les deux vice-présidents) a décidé de rendre publique cette décision en raison notamment du statut et de la taille de l'organisme en cause, et du nombre de personnes concernées par ses traitements.

Cette mise en demeure fait suite à la décision de Google Inc. de fusionner en une seule politique les différentes règles de confidentialité applicables à une soixantaine de ses services.

Dans sa décision, la présidente de la CNIL a notamment retenu que Google Inc. n'informait pas suffisamment ses utilisateurs sur les conditions dans lesquelles étaient collectées leurs données personnelles.

Il a également été reproché à la société, au terme d'un contrôle de proportionnalité entre, d'une part, son intérêt légitime et, d'autre part, les droits et intérêts des internautes, de ne pas avoir recueilli le consentement des utilisateurs avant de procéder à la combinaison de leurs données. La présidente a en effet retenu que l'ampleur et le caractère massif de la combinaison de données étaient susceptibles de méconnaître le droit des utilisateurs au respect de leur vie privée.

D'autres manquements relatifs à l'obligation de fixer une durée de conservation des données collectées ou encore d'informer les utilisateurs avant le dépôt de cookies sur leur terminal de connexion ont également été retenus.

La société ne s'étant pas mise en conformité avec cette mise en demeure, une procédure de sanction a été engagée. Le 3 janvier 2014, la formation restreinte de la CNIL a prononcé une sanction pécuniaire de 150 000 euros et a également enjoint à Google de procéder à la publication d'un communiqué relatif à cette décision sur www.google.fr.

Le 14 janvier 2014, Google a sollicité la suspension partielle de la délibération de sanction rendue à son encontre par la formation restreinte de la CNIL. Le juge des référés du Conseil d'État a rejeté cette demande par ordonnance en date du 7 février 2014.

Encadrer l'application extraterritoriale des lois d'États tiers impactant les citoyens européens

Les systèmes de surveillance de masse

Dès le mois de mars 2013, et avant même la publication des révélations d'Edward Snowden dans la presse, la CNIL a créé un groupe de travail chargé de mener des auditions et de réfléchir à la question de l'accès par des autorités étrangères aux données des citoyens européens.

La CNIL a participé activement aux travaux préparatoires du G29 sur les programmes de surveillance électronique de masse. À cet égard, elle a reçu ses homologues en juillet 2013 afin d'échanger sur ce sujet.

La présidente de la CNIL a également été auditionnée en octobre 2013 par la Commission LIBE du Parlement européen lors des discussions organisées sur la pertinence des outils juridiques d'encadrement des transferts dans l'affaire Prism.

Cette problématique n'est pas uniquement reliée à la protection des données, mais soulève des considérations excédant les limites des pouvoirs des autorités de protection des données nationales.

Pour ces raisons, la CNIL estime qu'une solution envisageable devrait être la création d'un outil spécifique, prenant la forme d'un accord international propre à garantir que les agences de renseignement de pays tiers offrent un niveau de protection adéquat.

Toutefois, en aucun cas un tel accord intergouvernemental ne pourrait légitimer un programme de surveillance électronique massive tel que Prism, dans les contours qui semblent être les siens compte tenu des informations rendues publiques. Un tel accord devrait en effet être conforme à la Charte des droits fondamentaux de l'Union européenne et à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). Ceci implique notamment que toute atteinte à la vie privée des citoyens doit être strictement et évidemment nécessaire, justifiée par un but légitime et proportionnée.

Par ailleurs, la CNIL soutient la réintroduction, dans le texte du projet de Règlement européen sur la protection des données, de l'ancien article 42 figurant dans le projet initial. Ce texte prévoyait en effet que les transferts de données vers des pays tiers à l'Union européenne opérés aux fins de répondre à une demande d'une autorité étrangère ne peuvent avoir lieu qu'avec l'autorisation de l'autorité nationale de protection des données.

Les listes noires

La CNIL a examiné plus précisément certaines lois créant et imposant aux administrations et aux entreprises l'obligation de vérifier la non-inscription de leurs salariés, fournisseurs ou sous-traitants sur des «listes noires» aux finalités diverses.

En effet, depuis plusieurs années, certains États, comme les États-Unis, cherchent à se prémunir contre divers risques (par exemple en matière de lutte contre le financement du terrorisme et d'exportations stratégiquement sensibles) au moyen de législations prévoyant des sanctions d'exclusion commerciale ou encore certaines restrictions.

La gestion de ces risques a donné lieu à la création et à l'utilisation de listes noires internationales ou nationales désignant certains États, personnes physiques ou morales, organismes ou groupes d'entreprises comme devant faire l'objet d'une sanction d'interdiction (par exemple, de commercer) ou comme devant faire l'objet d'une attention particulière. Ces législations imposent souvent que chaque opération impliquant directement ou indirectement ces pays, personnes, organismes ou groupes soit contrôlée.

La CNIL a commencé ses réflexions et recommande qu'un certain nombre de précautions minimales soient prises concernant l'utilisation de telles listes.

Les développements règlementaires

Les propositions sur les évolutions de la loi «informatique et libertés» dans le cadre d'un projet de loi sur le numérique

Suite à l'annonce du gouvernement, en février 2013, de déposer un projet de loi sur le numérique, la CNIL a formulé plusieurs propositions d'évolution législative qui pourraient être envisagées dans la perspective de ce projet.

Ces propositions concernent les quatre principaux acteurs de l'écosystème «informatique et libertés»: les individus, les entreprises, les pouvoirs publics, et la CNIL.

La CNIL propose notamment:

- un renforcement de l'effectivité des droits pour les personnes (ex.: exercice des droits par voie électronique…) et une protection particulière pour les mineurs;
- une poursuite de la simplification des formalités pour les entreprises;
- une extension du pouvoir de contrôle de la CNIL aux fichiers de renseignement, selon des modalités tenant compte de leurs spécificités;
- un accès direct aux données contenues dans les fichiers d'antécédents judiciaires pour les personnes non mises en cause à quelque titre que ce soit (victimes, plaignants);
- une augmentation du montant maximal des sanctions et une accélération du déclenchement d'une procédure de sanction pécuniaire.

La participation aux travaux sur la proposition de Règlement européen

Au regard de l'importance des enjeux, à la fois technologiques, politiques, économiques et internationaux, que représente le projet de Règlement, celui-ci a fait l'objet d'intenses débats en 2013 au Parlement européen comme au Conseil de l'UE.

Dans ce contexte, la CNIL a poursuivi sa démarche visant à sensibiliser les pouvoirs publics sur ses préoccupations.

Sur le guichet unique, la CNIL s'est attachée à promouvoir un modèle de gouvernance équilibré, dans l'intérêt de tous. Elle a ainsi conçu, en étroite collaboration avec le gouvernement français, une solution alternative et crédible au modèle de guichet unique tel que proposé par la Commission européenne. Cette proposition alternative repose sur les éléments suivants:

- une compétence conjointe et partagée sur les traitements «transnationaux» entre les autorités du pays de résidence des personnes visées par le traitement et l'autorité du pays de l'établissement principal de l'entreprise;
- une organisation de la coopération entre les autorités de protection par la désignation d'une autorité chef de file sur le critère de l'établissement principal;
- une adoption des décisions dans le cadre d'une procédure de codécision;
- un recours juridictionnel effectif, pour les personnes visées par le traitement, devant le juge de l'État de leur résidence contre les décisions de leur autorité et, pour les responsables de traitement, devant le juge de l'État de l'autorité chef de file dont dépend leur établissement principal;

- un nouveau rôle pour le Comité européen de la protection des données chargé de régler les différends entre les autorités de protection.

Sur les données pseudonymes, si la CNIL estime que la pseudonymisation des données, en tant que mesure de sécurité, peut justifier un régime d'obligations allégées pour les responsables de traitement, elle met toutefois en garde contre la création d'un régime dérogatoire pour les données pseudonymes en tant que telles.

Sur l'approche par les risques, la CNIL considère que l'approche par les risques ne doit en aucun cas affecter les droits ni conduire à exonérer le responsable de traitement (ou le sous-traitant) de son obligation générale de conformité aux dispositions du règlement.

Organisation	Autorité française de protection des données
Président et/ou collège	Président : Isabelle FALQUE-PIERROTIN Vice-présidents : Marie-France Mazars (depuis février 2014), Eric Peres (depuis février 2014). 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 2013 (en millions d'EUR) : 16,9
Personnel	Effectif : 178
Activités générales	
Décisions, avis, recommandations	2 452 décisions / 129 avis / 3 recommandations
Notifications	92 351 notifications à la CNIL, dont : 11 085 notifications pour des systèmes de vidéosurveillance 5 483 notifications pour des systèmes de géolocalisation 29 labels
Contrôles préalables	Autorisations : 2 615 en 2013, dont : 247 autorisations adoptées en séance plénière, 1 078 autorisations de transfert de données vers des états non membres de l'UE, 3 autorisations cadres, 416 autorisations de systèmes biométriques, 656 autorisations de traitement de données à caractère personnel à des fins de recherche médicale, et 215 autorisations de traitement de données à caractère personnel aux fins de l'évaluation ou de l'analyse de pratiques ou d'activités de soins et de prévention.
Demandes émanant de personnes concernées	Demandes émanant du public : En 2013, la CNIL a reçu 35 524 demandes par écrit et 124 595 appels téléphoniques

Plaintes émanant de personnes concernées	La CNIL a reçu 5 640 plaintes en 2013 Demandes émanant des personnes concernées : 4 305 demandes d'accès indirect où le traitement des données concerne la sécurité de l'État, la défense nationale ou la sécurité publique
Conseils sollicités par le Parlement ou le gouvernement	En 2013, la CNIL a adopté 129 avis. La CNIL a par ailleurs rencontré et été auditionnée à plus de 20 reprises par des parlementaires français pour un échange de vues sur des questions de protection des données.
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	414 enquêtes, dont 130 enquêtes relatives à des systèmes de vidéosurveillance.
Activités de sanction	
Sanctions	14 sanctions imposées par la CNIL en 2013. Actions en justice à l'encontre de responsables du traitement des données : 56 (57 mises en demeure, 7 sanctions financières, 5 avertissements), 1 relaxe.
Amendes	Amendes imposées par la CNIL en 2013 pour un montant total de 43 000 EUR
DPD	
Chiffres relatifs aux DPD	12 953 organisations ont désigné un DPD en 2013, pour un total de 3 679 DPD

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.

- CE, 10e sous-section, M. B. A. c/ Cnil 345408 (4/11/2013)
- CE, Juge des référés, SAS Paris Saint-Germain football & SASP Paris Saint-Germain handball c/ CNIL 373061 (20/11/2013)
- CE, Sous-sections 10 et 9 réunies, M. B. A. c/ CNIL, 328634 (3/06/2013)
- CE, Juge des référés, M. B. À 365459 (14 /02/2013)
- CE, Sous-section 10, Langlois, Association Internet sans Frontières, Société Ovh Sas c/ SGG, Ministère de l'Économie et des Finances 347349 (20/11/2013)
- CE, Sous-sections 10 et 9 réunies, M. A. / Conseil d'État 359417 (17 /07/ 2013)

- CE, Sous-sections 10 et 9 réunies, Société La Poste / Conseil d'État 342372 (17 /04/2013)
- CE, Sous-sections 10 et 9 réunies, Comité d'hygiène, de sécurité et des conditions de travail (CHSCT) de la société Lyondell Chimie France c/ Ministère de l'Intérieur 337982 (24/04/2013)
- Ccass Paris, Chambre commerciale, SARL Google France c/ société Cobrason 1121011112471394 (29/01/2013)
- Ccass, 1re Chambre civile, Société Agence du Palais c/ Rose Marie V, 1119530 (10/04/2013)
- Ccass, 1re Chambre civile, Société Google Inc. et autre c/ Société Lyonnaise de garantie 1217591 (19/06/2013)
- Ccass, Chambre commerciale, financière et économique, M. X. c/ société Bout-Chard 1217037 (25/06/2013)
- Ccass, Chambre criminelle, Mohamed X. c/ Ministère public 1381945 (22/10/2013)
- Ccass, Chambre criminelle, Société Biotronik France 1280346 (24/04/2013)
- Ccass, Chambre sociale, Association départementale pour la sauvegarde de l'enfance, de l'adolescence et des jeunes adultes des Alpes-Maritimes (ADSEA 06) c/ M. CARTON, 1126099 (23/04/2013)
- Ccass, Chambre sociale, M. Dubos c/ Société Distribution Casino France 1216564 (26/06/2013)
- Ccass, Chambre civile 1, Union fédérale des consommateurs de l'Isère c/ Caisse régionale de Crédit agricole mutuel Sud Rhône-Alpes 10283972 (23/01/2013)

GRÈCE

A. Résumé des activités et actualités

Le Parlement hellénique a adopté la loi anti-drogue nº 4139/2013, qui comprend, notamment, des dispositions relatives à la publication des données à caractère personnel des délinquants, et modifie par conséquent la loi nº 2472/1997 sur la protection des données à caractère personnel.

Au total, l'AHPD a émis cette année 158 décisions et 6 avis dont certains sont présentés à la section B « Informations sur la jurisprudence ».

L'AHPD a par ailleurs exprimé par écrit son avis sur a) le traitement de données à caractère personnel par des agences de notation de crédit, b) les deux projets d'accord, « Déclaration de protocole » et « Protocole d'accord », entre le conseil de supervision hellénique des normes de comptabilité et d'audit et le Public Company Accounting Oversight Board (PCAOB) américain pour l'échange transfrontalier d'informations sur la supervision des auditeurs, c) le plan d'action national pour un gouvernement hellénique ouvert dans le cadre de la participation de la Grèce au partenariat pour un gouvernement ouvert (OGP), et d) le programme « Cl@rity » (http://diavgeia.gov.gr/en) en vertu duquel tous les ministères et entités publiques en général sont tenus de publier leurs décisions sur Internet.

Lors de la journée européenne de la protection des données 2013, l'AHPD a publié sur son site Web la brochure et la vidéo « Prends le contrôle de tes données personnelles », créée par la Commission européenne (DG Justice), ainsi que des informations utiles sur la réforme de la législation applicable en matière de protection des données. À l'occasion de son 15e anniversaire et à des fins de sensibilisation, l'autorité a également organisé une conférence de deux jours dont le thème principal était la contribution de la DPA hellénique à la création d'un environnement favorable à la protection des données en Grèce.

L'autorité a également publié quatre numéros de son bulletin d'informations trimestriel sur l'évolution actuelle du domaine des données à caractère personnel aux niveaux national, européen et international. Enfin, l'AHPD a publié sur son site Web les résultats de l'enquête en ligne réalisée en 2012 sur des questions liées à la protection des données à caractère personnel.

Concernant les problèmes opérationnels de l'AHPD, une fois de plus, le sérieux problème du manque de personnel que l'AHPD connaît depuis sa création n'a pas pu être résolu au cours de l'année 2013 en raison des difficultés prolongées des finances publiques. En outre, la baisse continue du budget octroyé à l'AHPD à des fins opérationnelles a restreint les capacités de l'autorité à répondre de manière suffisante à ses obligations.

Organisation	
Président et/ou collège	Petros Christoforos (président du collège).
Budget	1 816 500 €.
Personnel	Département des auditeurs : 14 avocats et 11 experts informatiques (dont : trois (3) personnes en congé sans solde et deux (2) en congé maternité) ; département des communications et des RP : 5 (dont une (1) personne détachée une partie de l'année auprès d'un autre service de la fonction publique avant d'y être transférée, une (1) en congé maternité pour une partie de l'année et un (1) départ à la retraite) ; département des ressources humaines et des finances : 16 (dont une (1) personne transférée vers un autre organisme de la fonction publique, une (1) détachée à l'AHPD et

	transférée vers un autre organisme de la fonction publique et une (1) en congé maternité, ainsi que trois (3) transferts vers un autre organisme de la fonction publique, dont une personne (1) en congé sans solde).
Activités générales	
Décisions, avis, recommandations	L'AHPD a formulé 158 décisions et 6 avis.
Notifications	L'AHPD a reçu 650 notifications (381 concernant l'installation et le fonctionnement de caméras de télésurveillance et 92 transferts de données vers des pays en dehors de l'UE).
Contrôles préalables	L'AHPD a octroyé ou renouvelé 127 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 de personnes concernées	1 144.
Plaintes émanant de personnes concernées	692 (autorités judiciaires et ordre public : 20, administration publique et gouvernement local : 19, défense nationale : 5, ministère des finances-impôts : 3, santé : 5, sécurité sociale : 13, éducation et recherche : 9, banques : 111, économie privée : 107, communications électroniques : 264, relations de travail : 22, moyens de communication de masse : 3, autres : 111).
Conseils sollicités par le Parlement ou le gouvernement	4 – Cf. section (A) « Résumé des activités et actualités ».
Autres renseignements relatifs aux activités générales	Lors de la journée européenne de la protection des données 2013, l'AHPD a publié sur son site Web : la brochure et vidéo « Prends le contrôle de tes données personnelles », créée par la Commission européenne (DG Justice), des informations utiles sur la réforme de la législation sur la protection des données. À l'occasion de son 15e anniversaire et à des fins de sensibilisation, l'autorité a également organisé une conférence de deux jours (23-24 mai) à la salle de concert d'Athènes. Le thème principal en était la contribution de la DPA hellénique à la création d'un environnement favorable à la protection des données en Grèce. L'autorité a également publié quatre numéros de son bulletin d'informations trimestriel sur l'évolution actuelle du domaine des données à caractère personnel aux niveaux national, européen et international. Enfin, en 2013, l'AHPD a publié sur son site Web les résultats de l'enquête en ligne réalisée en 2012 sur des questions liées à la protection des données à caractère personnel.
Activités d'inspection	
Contrôles, enquêtes	10 contrôles auprès de responsables du traitement de données dans le secteur privé. Plus spécifiquement, quatre (4) ont été réalisés auprès d'entreprises afin d'enquêter sur leurs pratiques,

	plus particulièrement sur la licéité de la collecte et du traitement de données à caractère personnel dans le cadre de la prestation de services de notation de crédit. Deux (2) autres contrôles ont été réalisés auprès de deux banques au regard de violations de données présumées qui n'ont toutefois pas été confirmées. Deux (2) autres contrôles ont été réalisés sur l'envoi par deux sociétés de spams et de courriels non sollicités pour la promotion de services et de marchandises. Enfin, deux (2) enquêtes ont été réalisées sur le fonctionnement de systèmes de vidéosurveillance au sein d'une entreprise (une chaîne de livraison de pizzas) pour surveiller et contrôler le comportement et les performances des employés. L'autorité a également aidé l'unité anti-cybercriminalité de la police hellénique dans deux affaires (violation de données présumée au sein d'une société et traitement illégal de données à caractère personnel obtenues via un site Web).
Activités de sanction	
Sanctions	26 sanctions (6 avertissements, 20 amendes) ont été imposées par la DPA. Notons ici que, dans six (6) décisions, l'AHPD a imposé un avertissement et une amende. Les sanctions ont été imposées dans les domaines suivants : secteur public (3), marketing - promotion de biens et de services (3), secteur financier (4), violations de données à caractère personnel (2), moyens de communication de masse (1), vidéosurveillance (2), éducation et recherche (1) et communications électroniques (10).
Amendes	Amendes : le montant total des amendes imposées par la DPA hellénique s'élève à 311 735 €.
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

Avis 2/2013

Un avis a été délivré par l'AHPD au regard de la publication, sur le site Web du programme de mutuelle santé des journalistes (E.D.O.E.A.P.), concernant les dettes de personnes physiques en matière de cotisations d'assurance et de taxe sur la publicité. En réponse à une demande du programme de mutuelle santé des journalistes, l'autorité a jugé que la publication susmentionnée des dettes de personnes physiques sur Internet constituait une forme illicite de traitement de données à caractère personnel. Plus spécifiquement, cette approche n'est pas prévue par la loi ou un décret présidentiel et ne respecte pas non plus le principe de proportionnalité.

Avis 4/2013

L'autorité a jugé que la collecte et le traitement des extraits de casier judiciaire d'employés par la compagnie d'assurance pour laquelle ils travaillent, constitue une forme de traitement illicite, dans la mesure où cela ne respecte pas le principe de proportionnalité. L'autorité a, par ailleurs, jugé qu'une déclaration solennelle serait suffisante.

Avis 5/2013

L'autorité a examiné une demande du secrétaire général des recettes publiques concernant un projet de décision ministérielle sur le système de registres des comptes bancaires et de paiement, en cours de développement. Plus spécifiquement, ce système vise à faciliter le transfert des demandes de levée du secret bancaire des services et autorités judiciaires compétents aux établissements financiers, et la réception directe des réponses correspondantes sans intention de violer la législation sur la levée du secret bancaire et professionnel. L'AHPD a jugé que le traitement devait être prévu par une loi ou un décret présidentiel précisant le responsable du traitement, les objectifs, les données, la période de conservation, les destinataires des données, les spécifications techniques des applications requises pour le fonctionnement du système et les mesures organisationnelles et techniques mises en œuvre pour la sécurité du traitement de données à caractère personnel. L'autorité a également jugé que les « informations sensibles » devaient être effacées du système dès la réception de la réponse des autorités et services publics compétents, et que de plus amples mesures techniques devaient être appliquées pour s'assurer de la réception des réponses par les autorités qui en font la demande. Enfin, l'autorité a conclu que la solution la mieux appropriée pour la protection des données à caractère personnel et la proposition d'un recours efficace était que les établissements financiers et non le secrétariat général des systèmes d'information du ministère des finances (G.S.I.S.) soient obligés de conserver les données et que la période de conservation soit spécifiée afin de respecter le principe de recours efficace. Par ailleurs, le responsable du traitement devait aviser l'autorité du traitement prévu avant que celui-ci ne commence.

Décision 42/2013

Suite à des plaintes et après avoir réalisé des audits administratifs, l'AHPD a imposé une amende de 2 000 € à une société pour la collecte illégale et l'utilisation de données à caractère personnel à des fins de marketing direct et de publicité via l'envoi de communications électroniques non sollicitées. L'autorité a également imposé la destruction du fichier d'adresses électroniques. Le montant de l'amende a été déterminé en tenant compte, notamment, de la situation économique difficile de la société et de la coopération de ses représentants pendant l'audit administratif de l'autorité.

Décision 109/2013

Avec la décision 109/2013, la DPA hellénique a imposé une amende de 75 000 €à une banque pour avoir acheté et tenu à jour des dossiers de données à caractère personnel collectées illégalement pour ses activités promotionnelles. Les données étaient collectées sans le consentement des personnes concernées et n'étaient pas obtenues auprès de sources disponibles publiquement et destinées à fournir des informations au grand public. Par ailleurs, les personnes concernées n'avaient pas non plus divulgué leurs données à des fins similaires, sachant que la banque avait connaissance de l'ensemble de ces informations. L'autorité a également ordonné la destruction de toutes les listes concernées de la banque. Dans la même décision, l'AHPD a émis une recommandation afin que la banque respecte les dispositions de l'article 11 de la loi 3471/2006 sur la protection des données à caractère personnel et la vie privée dans le secteur des télécommunications électroniques, telle que modifiée et en vigueur, concernant la promotion de produits et de services, ainsi que les lois, règlements et instructions de l'autorité.

Décision 58/2013

L'AHPD a jugé que le traitement de données à caractère personnel simples et sensibles appartenant à des personnes en situation de handicap à des fins d'exemption du paiement des frais de péage constituait une forme légitime de traitement. Toutefois, la collecte et la tenue à jour de données à caractère personnel de personnes en situation de handicap dans le formulaire de demande d'exception tel qu'il était utilisé jusqu'à aujourd'hui, constituent une forme illicite de traitement de données à caractère personnel. La société devrait collecter moins de données à caractère personnel pour exempter

les personnes en situation de handicap du paiement des frais de péage, et également s'assurer que les personnes en situation de handicap soient informées de la collecte de données à caractère personnel et de la confidentialité et de la sécurité du traitement.

Décision 98/2013

L'AHPD a imposé l'amende la plus élevée possible au secrétariat général des systèmes d'information (G.S.I.S.) après avoir jugé que ce dernier violait son obligation de prendre des mesures de sécurité appropriées, ce qui a entraîné une fuite de données à caractère personnel particulièrement grave : cette violation des données concernait en effet presque tous les contribuables grecs. L'autorité a jugé que, malgré le volume des données dont il assure la gestion et leur nature sensible, le G.S.I.S. n'avait pas pris les mesures techniques et organisationnelles de sécurité appropriées pour éviter l'accès illégal et la diffusion de données avant juillet 2013, ni aucune mesure d'identification de potentielles violations des données à caractère personnel.

Décision 136/2013

L'autorité a jugé que la prestation du service Street View par Google, Inc. était licite, aux conditions visées dans la décision 53/2011, concernant le service Google Maps et autres conditions spécifiques, à savoir, d'informer les personnes concernées avant de commencer le traitement des données et respecter les droits d'accès et d'objection. Un délai de cinq jours a été donné à la société pour respecter ces droits.

Décision 138/2013

L'autorité a inspecté le système d'ordonnance électronique au regard de la protection et de la sécurité des données à caractère personnel. Le fonctionnement et la tenue à jour du système d'ordonnance électronique étant entièrement gérés par une société supervisée par le secrétariat général de la sécurité sociale (ci-après le « GGKA »), l'inspection s'est entièrement déroulée dans les locaux d'IDIKA et de ses sous-traitants. L'AHPD a demandé au responsable du traitement de données, le GGKA, de lui communiquer, dans les deux mois suivant la date de la décision, un calendrier détaillé de la mise en œuvre des recommandations visées aux motifs de la décision, et de résoudre les problèmes spécifiques mentionnés dans l'annexe confidentielle. Le calendrier devait également couvrir tous les recours prévus par l'actuel appel d'offres du nouveau système d'ordonnance électronique, qui n'a pas encore été attribué. L'autorité a, par ailleurs, demandé au responsable du traitement de lui adresser des rapports trimestriels sur l'avancement des travaux. Enfin, l'AHPD a demandé au responsable du traitement de décrire, dans sa demande de renouvellement d'autorisation du traitement de données sensibles, les nouvelles mesures qui auront été prises entretemps.

Systèmes de vidéosurveillance :

Décision 49/2013

Trois écoles privées avaient installé des systèmes de vidéosurveillance afin d'éviter les vols et le vandalisme dans leurs locaux et assurer la sécurité des élèves et des employés. Ces écoles souhaitaient exploiter leurs systèmes 24 heures sur 24 et ont demandé à être exclues de l'application de l'article 18 de la directive 1/2011 de l'AHPD sur l'installation de systèmes de vidéosurveillance, qui prévoit que, dans les écoles, ces systèmes ne puissent être exploités qu'en dehors des heures de travail. L'autorité a rejeté cette demande, dans la mesure où ces écoles n'avaient apporté aucune nouvelle suggestion justifiant la non-application de cette disposition. Ce qu'elles demandaient avait en outre déjà été pris en compte par l'AHPD au moment de rédiger la directive susmentionnée.

Décision 78/2013

Dans cette affaire, l'AHPD a été appelée à examiner la plainte d'un parent concernant un jardin d'enfants qui avait utilisé un système de vidéosurveillance dans les classes, la cour, le hall d'entrée et le bureau du directeur toute la journée, sans en avoir avisé les parents ou l'autorité. Le directeur de l'établissement a adressé une notification à l'AHPD et expliqué que ce système avait été installé parce que la zone à surveiller était très vaste, qu'il y avait eu plusieurs accidents avec des enfants et que les parents avaient été dûment informés. L'AHPD a jugé que le principe de proportionnalité n'avait pas été respecté et adressé un avertissement au jardin d'enfants lui enjoignant de désinstaller les caméras des classes, de s'assurer que les caméras de la cour étaient situées en périmètre de celle-ci, qu'il n'y avait pas d'écrans de contrôle et que les données seraient effacées d'une journée sur l'autre (sauf en cas d'incident). L'AHPD a, par ailleurs, conseillé au jardin d'enfants de respecter les droits d'accès et d'objection.

Décision 59/2013

Cette décision porte sur un système de vidéosurveillance installé dans un bâtiment public (une mairie) afin de protéger les propriétés publiques d'actes de vandalisme et, plus spécifiquement, plusieurs monuments alentour sérieusement endommagés ces deux dernières années. Le système a été jugé nécessaire en raison du fait que des mesures plus modérées avaient déjà été prises, telles qu'un meilleur éclairage et des patrouilles de police, sans avoir le résultat attendu. L'AHPD a invité le responsable du traitement à modifier le système de vidéosurveillance actuel de manière à i) ce qu'ils restent focalisés sur les monuments spécifiques, ii) retirer les écrans de contrôle et ne conserver que le système d'enregistrement, iii) ce que les mots de passe du système ne soient connus que d'une seule personne en particulier, nommée chef de la sécurité et de la vidéosurveillance, iv) ce que l'accès aux images et l'installation des écrans de contrôle ne soient possibles qu'en cas d'incident et sur ordre écrit du maire.

HONGRIE

A. Résumé des activités et actualités

En 2013, l'autorité nationale pour la protection des données et la liberté d'information (ci-après, la NAIH) a reçu plus de 3 000 soumissions. La plupart d'entre elles ont fait l'objet d'une enquête et d'une procédure informelle. La NAIH a lancé 40 procédures formelles (administratives) et imposé des amendes dans 31 cas. Certaines de ces décisions ont été contestées par les responsables du traitement de données devant un tribunal. Les tribunaux ont maintenu une vaste majorité des décisions examinées.

Organisation	Autorité nationale pour la protection des données et la liberté d'information
Président et/ou collège	Président : M. Attila Péterfalvi
Budget	467 500 000 HUF
Personnel	56
Activités générales	
Décisions, avis, recommandations	Décisions administratives En 2013, l'autorité a traité 40 affaires de protection des données. À l'heure de la rédaction du rapport annuel, 4 étaient encore en instance. 35 des 40 affaires de protection des données ont entraîné une décision administrative. Certaines de ces affaires étaient encore en instance fin 2013. Avis sur des projets de législation : 311 cas Avis sur l'enregistrement de voix : La NAIH a remarqué une augmentation des plaintes liées à des activités d'enregistrements vocaux. D'après la loi sur le respect de la vie privée, les enregistrements vocaux constituent des données à caractère personnel dans la mesure où il est possible de les associer à la personne concernée. Plusieurs lois prévoient l'obligation d'enregistrer certaines conversations vocales. La loi CCXXXVII de 2013 sur les établissements de crédit et les entreprises financières prévoit que ces établissements enregistrent les plaintes qui leur sont adressées par téléphone. Les compagnies d'assurance sont soumises à la même obligation d'après la loi LX de 2003 sur les établissements d'assurance et le secteur des assurances. Ces deux lois indiquent que les personnes concernées doivent pouvoir, si elles le souhaitent, écouter les enregistrements de leur voix. L'avis officiel de la NAIH est que chacune des parties a le droit d'accéder aux enregistrements vocaux. L'accès de la personne concernée à ces enregistrements doit dès lors également lui être assuré. Elle doit pouvoir les écouter et en obtenir une copie gratuitement, en règle générale. Résolutions Notre autorité a émis 1 549 résolutions sur des questions spécifiques à la protection des données (procédures informelles).

Notifications	Nous avons adressé 11 686 notifications de traitement de données à caractère personnel au registre des traitements.
Contrôles préalables	Aucune donnée.
Demandes émanant de personnes concernées	Ces demandes d'intervention sont traitées comme des « demandes consultatives » qui couvrent les demandes de responsables du traitement de données et, sur les 932 demandes, 790 concernaient des problèmes de protection des données. 140 traitaient de questions liées à la liberté d'information.
Plaintes émanant de personnes concernées	La NAIH a reçu 1 239 plaintes émanant de personnes concernées. Sur ces 1 239 plaintes, 978 affaires concernaient des problèmes de protection des données, et 261 des questions liées à la liberté d'information.
Conseils sollicités par le Parlement ou le gouvernement	La NAIH est régulièrement consultée sur des projets législatifs.
Autres renseignements relatifs aux activités générales	Affaires internationales : 106
Activités d'inspection	
Contrôles, enquêtes	Procédures de protection des données Les procédures de protection des données formelles sont lancées d'office. Dans la plupart des cas, les procédures formelles font suite à des procédures d'enquête informelles. Les informations recueillies lors de ces dernières peuvent être utilisées dans le cadre de procédures formelles. Stratégie d'enquête pour 2013 L'autorité a désigné trois domaines d'importance particulière et prioritaires en 2013 : 1. Les opérations de traitement de données par les sites Web, y compris le processus d'inscription du point de vue des droits des utilisateurs. Un accent particulier a été mis sur le traitement des données à caractère personnel des enfants. 2. La divulgation électronique des informations sur les impôts locaux. 3. Les opérations de traitement de données à caractère personnel par les sociétés de gestion des dettes. Enquêtes Le département des enquêtes a pour principale mission d'enquêter sur les plaintes déposées. Il répond également aux demandes de consultation qu'il reçoit afin d'aider à la mise en œuvre des lignes directrices sur la protection des données.

	Audits En 2013, l'autorité a lancé son service d'audit sur la protection des données. Les responsables du traitement de données peuvent, en contrepartie du paiement d'une redevance, demander un audit. La NAIH a réalisé 10 audits en 2013.
Activités de sanction	
Sanctions	La NAIH peut imposer plusieurs types de sanctions. Lors des procédures informelles, la NAIH peut demander au responsable du traitement de mettre ses procédures en conformité avec la loi sur le respect de la vie privée. Pendant les procédures formelles, la NAIH peut ordonner la rectification de toutes données à caractère personnel jugées imprécises, le blocage, la suppression ou la destruction de données à caractère personnel traitées de manière illicite, interdire le contrôle ou le traitement illicite de données à caractère personnel, interdire le transfert de données à caractère personnel vers d'autres pays ou ordonner la communication des informations de la personne concernée en cas de refus illicite du responsable du traitement de données, et imposer une amende.
Amendes	L'application d'amendes administratives fait partie des responsabilités de l'autorité. Principaux chiffres liés à cette activité en 2012-2013 : Nombre de cas 47 : Amendes imposées : 20 677 478 HUF
DPD	Depuis 2012, conformément à ses obligations légales, la NAIH organise au moins une fois par an une conférence des délégués à la protection des données internes.
Chiffres relatifs aux DPD	La DPA tient un registre des DPD. En 2013, plus de 400 DPD étaient enregistrés dans la base de données qui sert à inviter toutes les DPD intéressés à la conférence.

B. Informations sur la jurisprudence

Cas pertinents

A) Enquêtes sur des opérations de traitement de données par des sites Web, des processus d'inscription, et l'application des droits des personnes concernées sur Internet, en particulier ceux des enfants

La NAIH a entrepris une enquête globale sur les opérations de traitement de données par certains sites web afin d'évaluer les politiques relatives à la vie privée, les processus d'inscription, l'étendue des données traitées et l'application des droits des personnes concernées. Dans le cadre de cette procédure, la NAIH a accordé une attention particulière au traitement des données des enfants. L'importance accordée aux mineurs en tant que personnes concernées lors de notre procédure est justifiée par le fait que, contrairement à l'ancienne loi sur la protection des données, la nouvelle loi sur le respect de la vie privée, à son article 6, paragraphe 3, prévoit que les enfants de plus de 16 ans ont le droit de consentir au traitement de leurs données indépendamment de leurs tuteurs légaux.

Afin de déterminer la validité des déclarations légales et du consentement des mineurs à la collecte de données, il est également nécessaire de prendre en compte la loi IV de 1959 du Code civil (ci-après, le « Code civil »). Conformément à l'article 12/C, paragraphe 1, du Code civil, seul le tuteur légal d'un mineur, en sa qualité de représentant légal, peut faire des déclarations légales en son nom. Conformément à l'article 12/A, paragraphe 2, du Code civil : « les déclarations légales de mineurs dont les capacités légales sont limitées ne sont valides que si elles sont accompagnées du consentement préalable ou ultérieur de leur tuteur légal, sauf disposition contraire d'autres lois ». Ce type de dérogation est prévu à l'article 6, paragraphe 3, de la loi sur le respect de la vie privée. Avec cette disposition, le législateur a créé des règles spéciales pour les mineurs de 16 à 18 ans, mais pour les mineurs de 14 à 16 ans, le consentement de la personne concernée et de son tuteur légal reste nécessaire, conformément à la règle principale du Code civil.

La NAIH a rencontré le cas d'une société opérant plusieurs types de sites web, dont des sites de rencontre où l'on pouvait trouver des utilisateurs de moins de 16 ans qui avaient pu s'inscrire sans le consentement préalable ou ultérieur de leur tuteur légal. La NAIH a enquêté sur plusieurs sites de rencontre et observé que l'on y trouvait fréquemment inscrits des mineurs de moins de 16 ans. Selon la NAIH, il est important de prendre en compte les intérêts supérieurs des enfants lors de l'examen de leurs activités en ligne et des opérations de traitement qui les concernent et, notamment, dans le cas des réseaux sociaux. Dans cette catégorie, les sites de rencontre représentent la menace la plus importante. En effet, au contraire des réseaux sociaux habituels, où les utilisateurs communiquent essentiellement avec des amis qu'ils connaissent, la principale fonction des sites de rencontre est de rencontrer de nouvelles personnes. Étant donné que les services fournis par les sites de rencontre aux mineurs, et les opérations de traitement de données qu'ils impliquent, n'entrent pas dans la catégorie des activités quotidiennes anodines, normales et nécessaires pour répondre aux besoins de base d'un enfant, la NAIH pense que le consentement adéquat ne peut être constitué qu'avec celui du tuteur et non se composer uniquement de celui de l'enfant.

Il convient de tout faire pour que s'appliquent les règles susmentionnées, même s'il est vrai qu'il est difficile de vérifier le consentement des parents. Le propriétaire ou l'opérateur du site web facilite par ailleurs la disponibilité des enfants pour des relations romantiques ou sexuelles, ce qui peut contribuer à leur victimisation.

Nous ne pouvons fermer les yeux sur le fait que des enfants puissent apparaître sur des sites de rencontre et sur des sites web créés pour promouvoir l'établissement de nouvelles relations. Nous ne pouvons ignorer et, par conséquent, approuver passivement, de telles pratiques. Une réaction affirmée est nécessaire malgré le fait reconnu que les règles et processus d'inscription peuvent facilement être contournés. Dans ce cas, le problème ne relève pas du comportement du responsable du traitement de données, mais du domaine des relations parents-enfants, et d'un problème social plus large.

C'est pourquoi la NAIH a enquêté sur les processus d'inscription de pas moins de 50 sites de rencontre. La NAIH a essayé d'établir s'il était possible ou non pour des mineurs de s'inscrire sans le consentement de leurs parents. Au cours de nos inscriptions tests, la NAIH a été amenée à lancer des procédures administratives de protection des données à l'encontre de 18 sites web. Au total, nous avons identifié environ 4 200 profils de mineurs de moins de 16 ans. L'utilisateur le plus jeune n'avait que 10 ans. L'ensemble de ces profils étaient disponibles en ligne dans le but d'établir des relations. La NAIH a par conséquent imposé des amendes pour un montant s'élevant à 2 900 000 HUF au total, et forcé les responsables du traitement de données à effacer les données en question et à modifier leurs politiques en matière de protection des données.

Au cours de ces procédures, les responsables du traitement de données ont globalement été coopératifs, et ont supprimé les données à caractère personnel illégalement traitées, à savoir, les profils des mineurs de moins de 16 ans. Ils ont modifié leurs procédures et relevé l'âge d'inscription en conséquence.

B) Développement d'une base de données marketing commune

La NAIH a enquêté, dans le cadre d'une procédure administrative de protection des données, sur les opérations de traitement des données de deux sociétés gérant des bases de données marketing. La source des données collectées était l'inscription aux sites web des sociétés. Les deux sociétés transféraient et partageaient les données collectées entre elles, et envoyaient des courriels et des SMS aux utilisateurs inscrits. Les activités de télémarketing étaient menées depuis le centre d'appels d'un sous-traitant. Leur objectif était de faire la publicité de produits bancaires et d'assurance. Leur partenaire appelait les gens en utilisant l'identité de la société afin de promouvoir ses propres offres ou celles d'autres personnes inscrites dans l'une des bases de données des deux sociétés. Les données à caractère personnel étaient par conséquent reçues et utilisées par le centre d'appels et non par les responsables du traitement de données ayant collecté les données à l'origine.

La NAIH a établi que les opérations ayant fait l'objet de cette enquête ne respectaient pas de manière adéquate les exigences en matière d'information, et que le but indiqué des opérations (« à des fins de marketing ») était trop vague. Il n'existait aucune base juridique telle que le consentement des personnes concernées, par exemple, pour le transfert de données à caractère personnel par les sociétés à un partenaire dont le nom n'apparaissait même pas dans les conditions générales. Les deux responsables du traitement de données ne fournissaient pas non plus d'informations adéquates et précises, et n'offraient pas la possibilité d'adhérer délibérément. La notification adressée à la NAIH à des fins d'inscription préalable ne mentionnait pas tous les agents impliqués.

Compte tenu des violations établies, la NAIH a décidé d'imposer une amende, de demander l'adaptation des politiques relatives à la vie privée et des pratiques en matière de protection des données aux exigences de la loi sur le respect de la vie privée, et d'ordonner la suppression des données collectées illégalement.

C) Violation de données suite à une attaque de pirates

Une société collectait des données à caractère personnel dans le cadre d'un jeu de loterie à des fins de marketing direct, avec le consentement des personnes concernées. Sur son site web, la société donnait également accès à un jeu en 3D à ses utilisateurs inscrits. Une fois la campagne marketing terminée, le responsable du traitement des données a laissé un lien actif vers la base de données de son site web. Un groupe de pirates s'est introduit dans le serveur de la base de données. Ce groupe a ensuite téléchargé les données volées sur plusieurs sites web avec les noms, adresses électroniques, numéros de téléphone, dates de naissance, noms de villes et, dans certains cas, mots de passe de plus de 50 000 personnes.

Compte tenu de l'importance économique du responsable du traitement des données, la NAIH a considéré qu'il était de sa responsabilité de mettre en œuvre les mesures de sécurité des données les plus efficaces. Cette charge a été aggravée par le fait que des audits internes avaient déjà attiré l'attention sur la protection inadéquate de ces données, en particulier en matière d'accès à distance.

D) Systèmes biométriques

Certaines des affaires relatives aux systèmes biométriques concernaient des demandes de consultation par des organisations envisageant l'introduction de verrous ou de systèmes d'entrée biométriques. Conformément à son point de vue habituel, la NAIH a souligné que, compte tenu de l'article 4 de la loi sur le respect de la vie privée, il était nécessaire que l'emploi de systèmes biométriques soit adéquat, pertinent et proportionné. Ceci comprend les exigences applicables à la nécessité d'utiliser ces données, la proportionnalité de cette utilisation, et l'évaluation stricte de la question de savoir s'il serait possible ou non d'atteindre le même objectif par d'autres moyens moins intrusifs. La NAIH a par ailleurs continué de s'appuyer sur les conclusions de l'avis 03/2012 du groupe de travail « Article 29 » sur l'évolution des technologies biométriques et, notamment, sur les conclusions relatives à la manière dont la

proportionnalité de ces opérations de traitement devrait être analysée. D'après ces principes, les projets des écoles souhaitant introduire des systèmes d'entrée biométriques sont une source d'inquiétudes permanentes. En effet, ces systèmes ne sont pas indispensables pour la sécurité des parties concernées ou des biens des écoles. Enfin, il est possible d'atteindre la finalité souhaitée de ce type de système par des moyens moins intrusifs.

La NAIH a également examiné des cas d'entreprises ayant souhaité mettre en œuvre un dispositif relativement courant, un lecteur d'empreintes digitales, sur des caisses enregistreuses, afin d'en limiter l'accès au personnel autorisé. La NAIH a rappelé à ces sociétés que, d'après l'article 10, paragraphe 1, du Code du travail, « seules les déclarations ou les données pertinentes à l'établissement de relations de travail, l'accomplissement de cette relation ou sa cessation, peuvent être demandées à un employé, et seulement dans la mesure où ces demandes ne constituent pas une violation de ses droits civils ».

L'article 9 du Code du travail définit les règles générales et les principes fondamentaux de l'étendue des droits civils des employés dans les relations de travail, et de leurs potentielles restrictions. Afin de protéger ces droits civils, la loi prévoit que les employeurs respectent deux obligations procédurales strictes. Cette procédure doit être exclusivement et directement liée au fonctionnement propre à l'employeur et ne saurait dépasser ces limites. Même la notion de fonctionnement propre doit faire l'objet d'une interprétation stricte. L'employeur ne peut décider d'appliquer une telle procédure que si elle s'avère évidemment et objectivement nécessaire.

Sur la base de ce qui précède, la NAIH a établi que la mise en place de lecteurs d'empreintes digitales sur des caisses enregistreuses n'était pas proportionnée, la finalité souhaitée pouvant être atteinte par le biais de moyens moins intrusifs en termes de droits civils, tels que l'ouverture des caisses enregistreuses au moyen d'un code spécial donné par l'employeur aux seuls employés autorisés.

C. Autres informations importantes

Statistiques

En 2013, l'autorité a reçu plus de 5 700 courriers postaux et 11 222 courriers électroniques. Nous avons également traité 11 686 notifications de traitement de données à caractère personnel, dont 7 420 sont arrivées par courrier postal, et 4 266 par courrier électronique. Nous avons ouvert 3 280 dossiers en 2013, ce qui représente une augmentation de 9 % par rapport à 2012. Parmi ces dossiers, nous avons lancé 40 procédures administratives et 2 481 procédures d'enquête. Les 759 autres dossiers concernaient d'autres branches de nos activités, telles que les affaires internationales ou les relations avec les délégués à la protection des données. Seulement 370 des dossiers ayant fait l'objet d'une enquête commencée en 2012 se sont poursuivis en 2013. En janvier 2014, le nombre de dossiers non clos par rapport à l'année précédente a baissé à 341. Nous avons réussi à terminer 90 % de nos procédures en 2013, un résultat significatif dans un contexte d'augmentation du nombre de cas à traiter. Nous avons également traité 106 affaires internationales.

« La clé de l'univers d'Internet ! » : le projet de la NAIH pour la protection des enfants

En 2013, la NAIH a lancé son premier projet à long terme. Il concerne l'une de nos principales priorités : la protection des droits des enfants en ligne. La première étape de ce projet consistait à réaliser une étude exhaustive de l'utilisation d'Internet par les jeunes, des dangers auxquels ils sont confrontés en ligne, et de la réglementation juridique pertinente en Hongrie et à l'étranger. Nous avons mené cette étude en coopération avec plusieurs partenaires nationaux et internationaux. Notre but était d'inclure dans notre travail l'aide d'experts dans les domaines de l'éducation, de la psychiatrie, du droit, de la criminologie et des technologies de l'information, et d'obtenir des informations sur les meilleures pratiques internationales. Pas moins de 12 experts ont participé à la rédaction et à la publication d'une étude de 122 pages, et une brochure informative a été conçue pour les enfants et présentée dans

plusieurs écoles de Hongrie. Ce document a été traduit en anglais et un bref résumé a également été préparé en français. Tous deux sont téléchargeables librement sur notre site web : www.naih.hu. Notre but est de poursuivre ce projet avec nos partenaires internationaux dans le cadre d'un atelier international sur l'éducation numérique, sous la direction de la Commission nationale de l'informatique et des libertés (CNIL, France), ainsi qu'un projet financé par l'Union européenne appelé « Introducing data protection and privacy issues at schools in the European Union » (introduction des questions liées à la protection des données et de la vie privée dans les écoles de l'Union européenne), sous la direction de l'inspecteur général polonais pour la protection des données (GIODO).

IRLANDE

A. Résumé des activités et actualités

En 2013, le bureau du commissaire à la protection des données a ouvert 910 dossiers de plaintes à des fins d'enquête (de nombreuses plaintes sont traitées de manière informelle en fournissant au plaignant les informations appropriées quant à ses droits). 1 290 enquêtes sur des plaintes ont été conclues en 2013. Comme les années précédentes, la grande majorité des plaintes ont été réglées à l'amiable, 29 plaintes seulement ayant donné lieu à des décisions formelles. Les premières poursuites ont été engagées contre des sociétés pour des délits de marketing en vertu de la réglementation relative au respect de la vie privée dans les communications électroniques (décret-loi 336 de 2011 qui transpose la directive 2002/58/CE, telle que modifiée par les directives 2006/24/CE et 2009/136/CE en Irlande). Des informations relatives aux poursuites engagées en 2013 figurent à la section B du présent rapport. Le nombre de notifications de violations de la sécurité de données à caractère personnel adressées au bureau a peu évolué (1 507 en 2013), reflétant une tendance qui fait suite à l'introduction du code de bonnes pratiques en matière de violations de la sécurité des données à caractère personnel en 2010. Dans le cadre d'une violation importante de la sécurité de données impliquant un sous-traitant basé en Irlande et ayant des contrats avec plusieurs responsables du traitement des données à travers l'Europe, le commissaire a émis un avis d'exécution qui empêche le sous-traitant concerné de traiter des données tant qu'il n'a pas satisfait à certaines exigences en matière de sécurité des données. Le bureau a également mis en œuvre un formulaire en ligne afin de permettre le signalement de notifications de violation par des opérateurs de télécommunications et fournisseurs de service Internet, conformément aux exigences du règlement 611/2013 de la Commission européenne.

Organisation	Bureau du commissaire à la protection des données
Président et/ou collège	Billy Hawkes
Budget	1 727 000 € de budget. 1 960 999 € dépensés.
Personnel	30 au 31 décembre 2013.
Activités générales	
Décisions, avis, recommandations	29 décisions formelles
Notifications	5 778
Contrôles préalables	S. o.
Demandes émanant de personnes concernées	12 000 demandes par courriel. Demandes également reçues par écrit.
Plaintes émanant de personnes concernées	910
Conseils sollicités par le Parlement ou le gouvernement	Consultations informelles régulières sur des propositions législatives/réglementaires
Autres renseignements relatifs aux activités générales	1 507 notifications de violations de la sécurité des données.

Activités d'inspection	
Contrôles, enquêtes	44 audits (contrôles)
Activités de sanction	
Sanctions	101 poursuites engagées contre 14 entités
Amendes	35 600 € d'amendes imposées plus les coûts. 27 750 € de dons caritatifs ordonnés par le tribunal par l'application de la loi sur la probation, plus les coûts.
DPD	S. o.
Chiffres relatifs aux DPD	

B. Informations sur la jurisprudence

Dans la plupart des cas, conformément à la section 10 des lois irlandaises de 1988 et 2003 sur la protection des données, les plaintes déposées auprès du commissaire sont résolues à l'amiable sans qu'il soit nécessaire de recourir à une décision formelle ou une mesure coercitive. Ces règlements à l'amiable peuvent, par exemple, impliquer le versement d'une contribution financière par le responsable du traitement des données pertinent à la personne concernée ou à une œuvre caritative appropriée. Si nécessaire, des pouvoirs coercitifs sont appliqués, par exemple lorsque les responsables du traitement des données ne respectent pas les droits d'accès des personnes concernées. Dans un cas (mentionné à la section A ci-dessus), un avis d'exécution a été émis afin d'empêcher le sous-traitant de données de traiter des données tant qu'il n'avait pas satisfait à certaines exigences en matière de sécurité des données. Dans certains cas, les responsables du traitement des données sont nommés dans des études de cas incluses dans le rapport annuel du commissaire. En 2013, le commissaire a entamé avec succès plusieurs actions en justice en rapport avec le décret-loi 336 de 2011 (transposant la directive 2002/58/CE, telle que modifiée par les directives 2006/24/CE et 2009/136/CE en Irlande), concernant des SMS et courriels marketing non sollicités. 101 poursuites ont été engagées à l'encontre de 14 entités en 2013.

C. Autres informations importantes

Le commissaire a poursuivi son engagement auprès de grandes organisations du secteur public sur la protection des données. Le bureau a désormais terminé les audits de trois grands détenteurs publics de données à caractère personnel – le département de la protection sociale, l'administration fiscale et An Garda Síochána (forces de police nationales).

Un audit de la protection des données au sein d'An Garda Síochána a eu lieu entre 2011 et octobre 2013. Le rapport a été publié par An Garda Síochána en mars 2014. L'audit avait pour sujet central le principal système informatique PULSE, utilisé par An Garda Síochána pour enregistrer les données.

Les conclusions de l'audit ont mis en lumière des domaines où des améliorations étaient requises. Globalement, la plupart des examens ont permis d'observer que les forces de police professionnelles opéraient en conformité avec la législation sur la protection des données.

En 2013, le bureau a également commencé un vaste audit de LinkedIn Irlande.

ITALIE

A. Résumé des activités et actualités

Modifications de la législation

Code de protection des données (décret législatif nº 196 du 30 juin 2003)

La section 19, paragraphe 3-bis, du code de protection des données a été remplacée par la section 53(1)(e) du décret législatif nº 33 du 14 mars 2013. Toutefois, la formulation du paragraphe en question a été reprise à la section 4(5) dudit décret législatif (« Les informations concernant l'exécution des tâches confiées à toute personne en charge de fonctions publiques, y compris l'évaluation respective, devront être mises à disposition par l'employeur public. Sauf dispositions contraires de la loi, aucune information ne peut être divulguée sur la nature des pathologies et/ou des circonstances personnelles ou familiales résultant de l'absence d'une personne à son travail, ni les éléments de l'évaluation ni aucune information sur la relation de travail entre l'employé public et l'employeur public susmentionnés s'ils conviennent à la divulgation de tout élément d'information visé en section 4(1)d. des présentes. »).

La version la plus récente du code de protection des données est disponible en anglais ici : http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf

Activités principales

Traitement des données dans le secteur public

La DPA a émis un avis (le 7 février 2013) sur le projet de décret législatif (adopté le 14 mars 2013 – nº 14) qui établit les obligations de transparence spécifiques aux organismes publics (via la publication sur leurs sites institutionnels, par exemple). L'autorité a signalé des points critiques du texte du projet et a avancé des suggestions spécifiques pour réconcilier la transparence et la protection des données à caractère personnel, telles que : éviter de diffuser des catégories particulières de données, à savoir celles qui ont trait à la santé de la personne ; empêcher les données publiées en ligne de pouvoir être récupérées par l'emploi de moteurs de recherche répandus tels que Google (l'emploi de moteurs de recherche internes est préférable) ; définir la période pendant laquelle la publication de données sur des sites web peut être considérée comme proportionnée à des fins de transparence ; limiter la publication de données concernant des employés du secteur public aux données strictement pertinentes ; limiter la publication de données relatives aux responsables politiques en tenant compte des exigences de proportionnalité.

Lutte contre l'évasion fiscale

La DPA, suite à des investigations spécifiques, a prescrit des mesures à adopter au regard du traitement réalisé par l'agence du revenu et visant à évaluer rapidement les revenus des particuliers afin de lutter contre l'évasion fiscale (21 novembre 2013). Ces mesures avaient vocation à s'assurer que l'activité anti-fraude en question était déployée dans le respect de la protection des données à caractère personnel ; il s'agissait en particulier d'ajustements spécifiques que l'agence devait faire concernant les critères de profilage des contribuables et de sélection des personnes faisant l'objet d'investigations ; des dispositifs étaient par ailleurs prévus concernant la qualité des données ; la conservation des données ; les informations à communiquer aux personnes concernées concernant le traitement des données et la possibilité d'être entendu par l'agence.

Justice

La DPA a établi des mesures et des dispositifs que les bureaux du ministère public devront mettre en œuvre pour améliorer la sécurité de toutes les données à caractère personnel qu'ils collectent et utilisent dans le cadre de communications interceptées (24 juillet 2013). Ces mesures incluent des mesures de sécurité physique (telles que l'accès aux locaux exclusivement par le biais de badges individuels associés à un code numérique ou à des dispositifs biométriques ; l'enregistrement de tous les accès ; la vidéosurveillance des locaux) et des dispositifs de sécurité informatique (tels que l'utilisation de postes de travail dédiés et de procédures d'authentification pour l'accès des opérateur aux systèmes et aux serveurs ; l'enregistrement de toutes les activités liées à l'interception ; la copie protégée par cryptage sur des supports amovibles ; le stockage crypté des dossiers originaux et des copies de sauvegarde ; l'utilisation de protocoles réseaux sécurisés pour les échanges de données entre autorités judiciaires et FSI).

Services du renseignement

Suites aux révélations d'Edward Snowden, un protocole d'accord a été signé par la DPA italienne et le département de la sécurité des informations de la présidence du Conseil des ministres (11 novembre 2013). Ce protocole d'accord vise à compléter les garanties des droits des personnes concernant le traitement de données à des fins de renseignement, notamment, en ce qui concerne le contrôle par l'autorité des services de renseignement et des mécanismes d'évaluation des activités de ces services vis-à-vis des bases de données du secteur public et des initiatives de cybersécurité (notamment en ce qui concerne l'accès aux bases de données d'organismes publics et l'accès à des fins de cybersécurité).

Marketing

La DPA est intervenue à plusieurs occasions dans le domaine du marketing. Elle a émis des lignes directrices sur le marketing et contre les spams (y compris les spams dits sociaux, le marketing viral et le marketing ciblé), définissant un ensemble consolidé de mesures et de précautions pouvant être utiles aux sociétés qui planifient une campagne marketing pour faire la publicité de leurs produits ou services, et à toute personne souhaitant refuser les publicités sans consentement (4 juillet 2013). La DPA a clarifié, dans une décision distincte, le fait qu'il suffisait d'obtenir le consentement une seule fois pour toutes les activités de marketing telles que l'envoi de publicités ou la réalisation d'études de marché ; le consentement prévu pour recevoir des messages promotionnels automatiques (par courriel ou SMS) s'applique également à ces messages s'ils sont envoyés par le biais de canaux plus respectueux de la vie privée, tels que les courriers papier ou les appels téléphoniques par le biais d'un opérateur, sous réserve que les utilisateurs soient informés de manière appropriée et aient la possibilité d'exprimer librement leurs préférences respectives (15 mai 2013). Des règles détaillées ont été fixées pour les organismes publics et privés qui prévoient de recourir à des centres d'appels sis à l'extérieur de l'UE. Outre le rappel des exigences à respecter pour le transfert de données à caractère personnel (en particulier les données de clients) vers des pays tiers, la DPA a ordonné aux responsables du traitement concernés de fournir des informations spécifiques à leurs clients et de leur proposer la possibilité de sélectionner des opérateurs sis en Italie pour les appels téléphoniques entrants (10 octobre 2013). Des mesures spécifiques ont été définies par l'autorité et soumises à consultation publique afin de prévenir les appels silencieux, qui représentent un problème important aux yeux des utilisateurs. Ces mesures comprennent, notamment, la cessation des appels silencieux (c'est-à-dire, lorsqu'aucun opérateur n'est disponible pour prendre l'appel) dans les 3 secondes après que l'utilisateur a décroché ; l'imposition d'un plafond de 3 appels silencieux tous les 100 appels (par campagne de télémarketing) ; l'interdiction de recontacter un utilisateur avant un délai d'une semaine après le dernier appel silencieux ; et le stockage des statistiques relatives aux appels silencieux pendant au moins deux ans à des fins de contrôle.

Profilage par les compagnies de téléphone

Les compagnies de téléphone ont été autorisées par la DPA à déployer des activités de profilage sur la base de données agrégées sur une courte période (deux jours plutôt qu'un mois comme c'était le cas

jusqu'ici). La principale raison sous-tendant cette décision était l'utilisation croissante d'options de portabilité du numéro et l'élargissement de la gamme des offres (et des profils) de données proposée aux clients. Les données agrégées en question comprennent les volumes de trafic de départ et d'arrivée (en minutes ou en octets), le nombre de recharges (par canal de ventes, à savoir en ligne, DAB, cartes de débit) et le nombre total de recharges. Toutes les autres garanties définies par la DPA dans de précédentes décisions restent applicables, y compris l'utilisation de systèmes informatiques dédiés pour le profilage, et de mesures de sécurité contraignantes pour l'accès aux données.

Paiements mobiles

La DPA a adopté une décision (le 12 décembre 2013) sur les paiements mobiles, imposant des garanties spécifiques pour protéger les données à caractère personnel des utilisateurs qui, en facturant directement leurs factures téléphoniques, font des paiements à distance à l'aide de systèmes de paiement à distance mobile. Ce mode de paiement est de plus en plus répandu et implique le traitement de plusieurs types de données à caractère personnel (parfois sensibles) telles que des informations démographiques, le type de service ou de produit acheté, et la date et l'heure de l'achat. Les garanties (qui incluent un avis d'information spécifique, le consentement en cas de marketing et de profilage, des mesures de sécurité et des politiques de conservation des données) sont de la responsabilité des trois principaux acteurs impliqués dans les services de paiement mobile (les opérateurs, c'est-à-dire les fournisseurs de communications électroniques ; les plateformes de paiement qui fournissent et gèrent les plateformes technologiques pour ces services ; et les marchands qui offrent et vendent des contenus numériques, multimédias et autres produits).

Google Street View

En décembre 2013, la DPA a imposé à Google une amende de 1 million d'euros pour son service Google Street View en particulier, pour un rassemblement d'informations collectées de manière illicite dans une grande base de données (créée par Google pour son service Street View). L'autorité a par ailleurs décidé de s'appuyer sur la disposition du code de protection de la vie privée qui vise à garantir que des sanctions efficaces soient imposées aux grandes entreprises commerciales (compte tenu du chiffre d'affaires consolidé de plus de 50 milliards de dollars enregistré par Google en 2012).

Violations de données

La DPA a adopté une décision générale qui remplace les lignes directrices précédemment adoptées, conformément au paragraphe (6) de la section 32-bis du code (qui met en œuvre la directive 136/2009/CE) afin de donner des conseils et des instructions sur les circonstances dans lesquelles les fournisseurs de services de communications électroniques doivent notifier les violations de données à caractère personnel, le format qui doit s'appliquer à ces notifications et les modalités d'application pertinentes (4 avril 2013).

Techniques d'authentification graphométrique

La DPA a accepté deux demandes de vérification préalable de la part de banques souhaitant utiliser des techniques d'authentification graphométrique pour l'identification de leurs clients. La DPA a demandé que le principe de limitation de la finalité soit strictement respecté et que des procédures alternatives soient disponibles pour les utilisateurs ne souhaitant pas et ne pouvant pas faire confiance à cette méthode d'authentification ; les dispositifs de conservation des données devront également respecter le principe de proportionnalité.

La dimension internationale

La DPA italienne a maintenu sa participation active au groupe de travail « Article 29 ». La DPA a également pu suivre les débats en cours sur la reformation de l'initiative-cadre européenne relative à la protection des données en participant grâce à ses experts à la délégation italienne auprès du groupe de travail DAPIX du Conseil de l'UE.

La DPA a contribué au travail de l'OCDE et du Conseil de l'Europe, en particulier via le groupe de travail sur la sécurité de l'information et la vie privée, ainsi que le comité consultatif et le bureau du T-PD, qui travaille actuellement à une révision de la Convention 108/1981. La DPA fait partie des autorités de contrôle communes au niveau européen (ACC d'Europol, ACC de Schengen, SID, groupe de coordination Eurodac). Elle participe et contribue également régulièrement au groupe de Berlin (groupe de travail international sur la protection des données dans les télécommunications).

Aux niveaux européen et international, l'année 2013 a également été caractérisée par le travail important effectué par les DPA en faveur d'une coopération plus étroite et plus efficace, surtout dans le domaine de la mise en application par le biais de groupes de travail spécifiques auxquels la DPA italienne a participé (GPEN, groupe de travail de la CEI, projet Phaedra, etc.). La DPA a poursuivi son travail dans le cadre des programmes IAP, TAIEX et de jumelage de la Commission européenne pour les nouveaux pays de l'UE, les pays candidats (Turquie, Croatie jusqu'en juin 2013, ARYM) et les pays adhérant à la politique européenne de voisinage.

Organisation	Autorité italienne de protection des données
Président et/ou collège	Président du collège : Dr Antonello SORO Collège : Mme Augusta IANNINI Mme Giovanna BIANCHI CLERICI Mme Licia CALIFANO
Budget	Environ 8,4 millions d'EUR (financés par le gouvernement)
Personnel	122
Activités générales	
Décisions, avis, recommandations	Nombre de décisions prises par le collège : 606
Notifications	1 656
Contrôles préalables	24
Demandes émanant de personnes concernées	Nombre total de demandes : environ 4 700 Demandes d'informations (« quesiti ») : 311 Signalements et réclamations (« segnalazioni » et « reclami ») reçus en 2012, émanant de personnes concernées : 4 393
Plaintes émanant de personnes concernées	(plaintes officielles, réglementées spécifiquement par le code de protection des données, concernant l'accès à ses propres données personnelles) : 222
Conseils sollicités par le Parlement ou le gouvernement	22
Autres renseignements relatifs aux activités générales	Les bureaux de la DPA ont reçu, en 2013, environ 31 000 appels téléphoniques et courriels

Activités d'inspection	
Contrôles, enquêtes	Nombre de contrôles et/ou d'enquêtes (sur place) : **411**
Activités de sanction	
Sanctions	Environ **850**
Amendes	Montant : environ **4 millions d'EUR** imposés par la police financière chargée des contrôles au nom de la DPA
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

Cour suprême – Affaire Google Vividown – Aucune responsabilité pénale d'un fournisseur de services d'hébergement

La troisième chambre pénale de la Cour suprême italienne (par sa décision nº 8611/2013) a publié la motivation de son verdict d'acquittement pour les trois dirigeants de Google qui avaient été condamnés à six mois de prison en première instance en 2010, suite au chargement, sur la plateforme vidéo de Google, d'un enregistrement où un mineur handicapé était humilié par ses camarades de classe. D'après la Cour suprême, les hébergeurs de sites web ne peuvent être tenus pénalement responsables en cas de violation de la vie privée due à des vidéos publiées sur le web. Cette décision très importante établit que « les délits qu'il nous est donné de juger, relativement à la section 167 du code de protection de la vie privée, sont interprétés comme des délits commis en violation d'obligations, étant entendu que nous nous trouvons face à un comportement ne donnant lieu qu'à une violation des obligations du propriétaire des données traitées et d'aucune autre personne qui manipule les données traitées de quelque manière que ce soit, sans disposer d'aucun pouvoir décisionnel y afférent ». La Cour suprême a également spécifié que le fournisseur de services d'hébergement « n'a aucun contrôle sur les données stockées ni ne contribue en aucune manière à la sélection de ces données, à leur recherche ou à la création du fichier qui les contient, ces données étant entièrement attribuables aux utilisateurs du service qui les ont chargées sur la plateforme mise à leur disposition ».

Cour de cassation (Cour suprême) – Le consommateur a le droit d'être informé sans délai des rapports négatifs qui le concernent

Une décision de la division civile de la cour de cassation (nº 349/2013) concernant les droits des consommateurs a conclu qu'un consommateur avait le droit d'être informé sans délai des rapports négatifs qui le concernent. La cour a déclaré inadmissible (pour des raisons liées aux services de traitement) l'action intentée par une société financière contre un jugement prononcé en première instance à Milan. Dans cette affaire, la personne concernée, ayant entendu parler d'un « rapport négatif » à son encontre quant à un prêt qui lui avait été octroyé en 2003, avait déposé une demande appropriée d'accès à la base de données de la société en 2008 et fait appel devant le tribunal de Milan après n'avoir reçu aucune réponse. La Cour suprême a confirmé le droit du consommateur de connaître sans délai sa situation dans les archives de la société financière, et souligné, notamment, que le responsable du traitement des données devait vérifier la demande de connexion « sans délai ». Par conséquent, le tribunal avait dûment tenu compte du délai de 15 jours prévu par la loi pour que le responsable du

traitement réponde aux demandes d'accès, et jugé que ce délai était adéquat pour que le responsable du traitement puisse prendre une décision de réponse à cette demande.

Cour de cassation (Cour suprême) – Interférence illicite avec la vie privée

La division pénale de la cour de cassation (par sa décision nº 8762/2013) a rejeté un appel contre la décision de la cour d'appel de Florence, qui avait condamné le défendeur pour violation de l'article 615-bis du code pénal italien après avoir pris connaissance d'une conversation entre sa sœur et sa petite amie dans son appartement en cachant un magnétophone dans ledit appartement. La cour, se référant à une jurisprudence constante, a déclaré que le délit d'interférence illicite dans la vie privée existait aussi dans le cas d'enregistrements abusifs tels que celui en question, et a souligné, à des fins d'applicabilité de l'article 615-bis du code pénal, que « le domicile (lieu d'habitation privé) d'une personne inclut le lieu où se déroule une part importante de sa vie émotionnelle, même si elle n'y réside pas constamment… ». La décision souligne que, dans ce genre de lieu, une personne est généralement convaincue que sa vie privée y est protégée, et se trouve par conséquent particulièrement exposée et vulnérable au comportement sournois et déloyal de la personne à laquelle il ou elle est émotionnellement lié.

C. Autres informations importantes

La DPA a manifesté son intérêt pour que l'État italien apparaisse devant la Cour de justice de l'UE dans l'affaire C-46/13 (demande de décision préjudicielle au titre de l'article 267 du TFUE) sur l'interprétation de l'article 7(c) de la directive 2006/24/CE. Les questions demandées par la commission autrichienne de la protection des données à la Cour de justice européenne devaient permettre de comprendre, notamment, si l'article 7(c) de la directive 2006/24/CE pouvait être interprété en ce sens qu'une personne concernée par des données conservées ne faisait pas partie de la catégorie du « personnel spécifiquement autorisé » au sens de cette disposition, et n'avait aucun droit d'accès à ses propres données envers le fournisseur de services de communications électroniques accessibles au public ou envers un gestionnaire d'un réseau public de communications. La DPA italienne a souligné que, conformément aux sections 7 et 8 du code italien de protection des données, les personnes concernées pouvaient avoir accès à toutes les données à caractère personnel les concernant telles qu'elles sont traitées par un prestataire de services, à l'exception des appels téléphoniques entrants, sauf si cet accès peut porter un préjudice réel et concret aux investigations de l'avocat de la défense.

LETTONIE

A. Résumé des activités et actualités

Pour les principaux développements, les modifications de la loi sur la protection des données à caractère personnel ont été élaborées (et sont entrées en vigueur le 7 mars 2014). Ces modifications prévoient une participation plus claire des personnes concernées au traitement des données à caractère personnel afin de résoudre les problèmes y afférents (par exemple, lorsque la personne concernée demande une grande quantité d'informations au responsable du traitement, etc.). Elles concernent également la vidéosurveillance : il est obligatoire d'aviser l'inspection nationale des données de ces traitements de données uniquement en cas de stockage de données à caractère personnel acquises via la vidéosurveillance. Des modifications apportées à plusieurs lois sectorielles ont augmenté la charge de travail de l'inspection nationale des données, principalement en ce qui concerne les notifications de vidéosurveillance à l'inspection nationale des données.

Étant donné l'utilisation de plus en plus répandue de la vidéosurveillance en Lettonie, l'inspection nationale des données de Lettonie a initié une discussion plus vaste sur ce sujet avec le bureau du médiateur.

Organisation	INSPECTION NATIONALE DES DONNÉES
Président et/ou collège	Directeur – Signe Plūmiņa
Budget	En 2013 – 265 317 LVL (ou 377 512 EUR)
Personnel	19 (personnel administratif compris)
Activités générales	
Décisions, avis, recommandations	Décisions : pas de données statistiques disponibles ; avis : pas de données statistiques disponibles ; recommandations : 2
Notifications	532
Contrôles préalables	493
Demandes émanant de personnes concernées	6
Plaintes émanant de personnes concernées	362
Conseils sollicités par le Parlement ou le gouvernement	Pas de données statistiques disponibles ; les conseils au Parlement ou au gouvernement sont souvent donnés par le ministère de la justice qui y inclut également l'avis de l'inspection nationale des données.
Autres renseignements relatifs aux activités générales	8 décisions de fonctionnaires de l'inspection nationale des données ont fait l'objet d'un appel devant le directeur de l'inspection nationale des données. 4 décisions du directeur de l'inspection nationale des données ont fait l'objet d'un appel devant un tribunal.

	Principaux domaines des plaintes : Violations du droit d'accès des personnes concernées (concernant les informations à fournir au début du traitement des données à caractère personnel et les informations à fournir sur demande de la personne concernée) ; Vols d'identité (en ligne et hors ligne).
Activités d'inspection	
Contrôles, enquêtes	677 (dont seulement ~ 5 % sont des initiatives personnelles)
Activités de sanction	
Sanctions	Applications de sanctions administratives dans 36 cas : 14 avertissements et 22 amendes.
Amendes	20 476 55 LVL (29 135,50 EUR).
DPD	
Chiffres relatifs aux DPD	42 DPD désignés par les responsables du traitement

B. Informations sur la jurisprudence

Aucun accomplissement spécifique.

C. Autres informations importantes

Afin d'encourager la coopération, l'inspection nationale des données de Lettonie a participé à la réunion annuelle des trois États baltes, où la décision a été prise de réaliser une enquête annuelle conjointe sur la protection des données à caractère personnel dans les spas et les installations récréatives en 2014. Une enquête annuelle conjointe sur les établissements de jeux et les casinos a été conclue en 2013.

LITUANIE

A : Résumé des activités et actualités

Étant donné que la Lituanie a présidé le Conseil de l'Union européenne du 1er juillet au 31 décembre 2013, l'inspection nationale de protection des données de la République de Lituanie (ci-après l'INPD) a focalisé son attention sur la réforme de la protection des données, et a participé activement aux réunions du groupe de travail DAPIX.

La journée européenne de la protection des données a été célébrée le 25 janvier 2013. Une conférence de presse a été organisée au parlement lituanien lors la journée de la protection des données, sous le titre « Protection des données au sein de l'Union européenne et de la Lituanie ». Le 4 février 2013, la journée de la protection des données a été célébrée à l'école secondaire Mykolas Biržiška. L'INPD a organisé un séminaire pour les élèves de cette école sur le respect de la vie privée et la publicité dans la société de l'information, sur les passeports de la République de Lituanie, les réseaux sociaux et autres problèmes similaires.

L'INPD a activement participé à la conférence « Protection des données à caractère personnel : application aux personnes et aux entreprises », organisée par la confédération des entreprises de Lituanie le 9 mai 2013.

Les autorités de contrôle de la protection des données lettone, lituanienne et estonienne se sont rencontrées dans le but de poursuivre la coopération des États baltes en mars 2013 à Riga, en Lettonie. Les autorités de contrôle des données à caractère personnel des pays baltes ont mené une deuxième enquête conjointe sur le traitement et la protection de données à caractère personnel au sein du secteur du jeu. Au total, 13 casinos des pays baltes ont été inspectés en 2013.

Le système d'information « HELP » a été lancé en 2013, pour permettre l'accès à l'INPD via des réseaux de communications électroniques. Par conséquent, les personnes concernées et les responsables du traitement des données ont la possibilité de déposer des plaintes ou toute autre forme de demande auprès de l'INPD par voie électronique en tout lieu et à tout moment, et de recevoir une réponse par la même voie. Désormais, les personnes concernées et les responsables du traitement des données ont la possibilité de savoir qui est en charge de leur dossier, de quelle nature est la procédure et où en est leur dossier.

Algirdas Kunčinas a été désigné au poste de directeur de l'INPD pour un second mandat de cinq ans. Son nouveau mandat commencera le 1er janvier 2014.

Organisation	
Président et/ou collège	Dr Algirdas Kunčinas
Budget	1 919 000 Litas (555 781 euros)
Personnel	30
Activités générales	
Avis, recommandations	S. o.
Notifications	1 409
Contrôles préalables	338

Demandes émanant de citoyens	23
Plaintes émanant de citoyens	327
Conseils sollicités par le Parlement ou le gouvernement	S. o.
Autres renseignements relatifs aux activités générales	3 845 consultations ; 100 communiqués d'information au public ; 4 synthèses des résultats des enquêtes préventives et de la jurisprudence ; 29 conclusions sur les documents de l'UE et du Conseil de l'Europe ; 65 réponses à des demandes de parties à la Convention (STE nº 108) ; 309 actes juridiques coordonnés et documents de responsables du traitement des données ; 11 actes juridiques préparés ; et 6 consultations publiques.
Activités d'inspection	
Contrôles	51
Activités de sanction	
Sanctions	L'INPD a mis en place 41 protocoles pour des infractions administratives
Amendes	S. o.
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

Traitement d'un numéro d'identification personnel

Une personne a porté plainte parce qu'un fournisseur d'accès à Internet et de services de télévision par câble lui avait demandé de signer un contrat standard et d'écrire son numéro d'identification personnel dans le contrat. En vertu du paragraphe 2 de l'article 7 de la loi sur la protection juridique des données à caractère personnel de la République de Lituanie (ci-après, la LPJDP), l'utilisation d'un numéro d'identification personnel est autorisée lors du traitement de données à caractère personnel uniquement avec le consentement de la personne concernée. Le paragraphe 3 de cet article détermine des exceptions à la règle. L'INPD a déclaré que le consentement du plaignant n'était pas libre puisque, s'il ne le donnait pas, il ne pourrait pas bénéficier du service, et a donné à la société une instruction légalement contraignante de modifier la forme du contrat standard et de ne pas demander les numéros d'identification personnels de ses clients. Cette décision a fait l'objet d'un appel de la société devant le tribunal administratif de grande instance de Vilnius. Le tribunal a rejeté l'appel comme étant non fondé, et a conclu que la décision de l'INPD selon laquelle le consentement du plaignant n'avait pas été donné librement était correcte. Le plaignant a fait appel de cette décision devant la Cour administrative suprême, qui a également déclaré que l'instruction de l'INPD avait été correcte et que les arguments de la société selon lesquels le numéro d'identification personnel était nécessaire dans le contrat n'avaient aucune importance dans cette affaire.

Divulgation de données à caractère personnel aux médias

Une personne a déposé une plainte parce que l'inspection des impôts avait divulgué aux médias ses données à caractère personnel sur une enquête fiscale en cours. Conformément au paragraphe 1 de l'article 38 de la loi sur l'administration fiscale de la République de Lituanie, l'administrateur des impôts est tenu d'assurer la confidentialité des informations des contribuables et à ne les utiliser qu'à des fins licites. Conformément à l'alinéa 6 du paragraphe 2 de l'article 38 de cette même loi, la confidentialité des informations relatives aux violations des lois fiscales n'est pas garantie si la faute du contribuable en la matière est avérée. L'INPD a décidé que la divulgation, par l'inspection nationale des impôts, des données à caractère personnel du plaignant sur l'enquête fiscale non terminée était illégale en raison du fait qu'elle ne reposait sur aucun fondement juridique prévu à l'article 5 de la LLPDP ni sur aucun autre critère de divulgation licite des données à caractère personnel. L'INPD a donné pour instruction à l'inspection nationale des impôts de ne pas informer les médias (qui le demandent) des enquêtes fiscales encore en cours auprès de personnes physiques parce que la violation de la loi par le contribuable reste à prouver.

Cette instruction a fait l'objet d'un appel devant le tribunal administratif de Vilnius par l'inspection nationale des impôts, qui a plaidé que la divulgation de faits relatifs à une enquête fiscale commencée pouvait servir à prévenir les violations et à informer sur les activités de l'institution. Le tribunal a rejeté l'appel sur la base de l'article 38 de la loi sur l'administration fiscale et déclaré que la divulgation des données à caractère personnel d'un contribuable ne pouvait être justifiée par les objectifs de prévention des violations et d'information sur les activités de l'institution.

L'inspection nationale des impôts a fait appel de cette décision auprès de la Cour administrative suprême, qui a également rejeté cet appel.

LUXEMBOURG

A. Résumé des activités et actualités

Modifications de la législation

Aucune modification n'a été apportée à la législation dans le domaine de la protection des données et de la vie privée en 2013.

Principales questions abordées

L'une des missions de la CNPD est de conseiller le gouvernement du Luxembourg sur les sujets liés au respect de la vie privée et à la protection des données. 10 avis formels sur des lois et règlements ont été émis en 2013. Les principales questions abordées ont été les suivantes :

- l'organisation des services de renseignement nationaux ;
- le statut, la procédure de désignation et les pouvoirs du médecin coordinateur ;
- la réforme de la loi concernant les services publics ;
- la réforme sur l'exécution des sentences et l'administration pénitentiaire ;
- l'échange transfrontalier d'informations sur la sécurité routière relatives aux infractions routières ;
- le registre national du cancer.

Dans le domaine des systèmes intelligents de mesure, la CNPD aide Luxmetering à mettre en œuvre ses processus et procédures opérationnelles dans le cadre d'une évaluation de l'impact sur la vie privée (EIP). Luxmetering est un groupement d'intérêt économique composé de 7 gestionnaires de réseau d'électricité et de gaz luxembourgeois. Il est responsable de la mise en œuvre des infrastructures et du déploiement national d'environ 350 000 compteurs intelligents.

Actualités

La CNPD et la CNIL (France) ont réalisé une analyse du « contrat de services Microsoft » et de la « politique de confidentialité en ligne de Microsoft » à la demande du groupe de travail « Article 29 » après que l'entreprise a modifié ses conditions contractuelles d'utilisation. Des exemples précédents, où des entreprises telles que Google ou Facebook avaient modifié leurs conditions d'utilisation, ont montré que ces changements pouvaient avoir des effets conséquents en Europe et potentiellement affaiblir la protection des données à caractère personnel et de la vie privée des personnes.

Après les révélations parues dans la presse internationale concernant le programme PRISM, la DPA luxembourgeoise a reçu deux demandes de citoyens européens destinées à vérifier si Skype et Microsoft Luxembourg avaient traité leurs données de manière licite et si les sociétés avaient partagé leurs données avec la NSA, l'agence nationale de sécurité américaine.

En tant que DPA chef de file, la CNPD a approuvé les BCR du groupe sidérurgique multinational ArcelorMittal sis au Luxembourg, après 18 mois de discussions avec les DPA des 25 autres pays européens où le groupe ArcelorMittal est présent. Il s'agissait de la deuxième procédure d'approbation de BCR pour la CNPD, qui avait déjà agi en tant que DPA chef de file pour les BCR d'eBay en 2009.

Principaux événements et activités de sensibilisation

Pour célébrer son 10e anniversaire, la CNPD a organisé une conférence le 28 janvier 2013 (pour la journée de la protection des données) en présence de Dean Spielmann (président de la Cour européenne des droits de l'homme) sur le sujet de « *la protection des données dans la jurisprudence de la Cour européenne des droits de l'homme* ».

Outre cet événement important, la DPA luxembourgeoise a participé à plusieurs événements de sensibilisation destinés au grand public ainsi qu'à des séminaires et formations visant un public plus spécialisé. La CNPD a également participé à la conférence des délégués à la protection des données organisée par l'AFCDP (Association française des correspondants à la protection des données à caractère personnel) au Luxembourg.

Organisation	Commission nationale pour la protection des données (CNPD)
Président et/ou collège	M. Gérard LOMMEL – Président M. Thierry LALLEMANG — Commissaire M. Pierre WEIMERSKIRCH — Commissaire
Budget	1 552 000 €
Personnel	Collège : 3 Service juridique : 5 Notifications et contrôles préalables : 2 Administration générale : 2 Communication et documentation : 1 Informatique et logistique : 1 Total : 14
Activités générales	
Décisions, avis, recommandations	693
Notifications	1 072
Contrôles préalables	725
Demandes émanant de personnes concernées	270
Plaintes émanant de personnes concernées	177
Conseils sollicités par le Parlement ou le gouvernement	10
Autres renseignements relatifs aux activités générales	Réunions et consultations (avec les secteurs public/privé) : 177

	Conférences et réunions d'information : 18
Activités d'inspection	
Contrôles, enquêtes	26
Activités de sanction	
Sanctions	1
Amendes	S. o.
DPD	
Chiffres relatifs aux DPD	DPD désignés en 2013 : 20 Nombre total de DPD désignés (à la date du rapport) : 49

B. Informations sur la jurisprudence

Tribunal de première instance, chambre du travail, 7 mars 2013, sur la validité de preuves (correspondance électronique) collectées en l'absence d'autorisation préalable de la CNPD

Dans cette affaire, la principale question consistait à déterminer si le licenciement avec effet immédiat d'un employé de la société X devait être considéré comme excessif ou justifié. L'employeur avait évoqué des pratiques de concurrence déloyale de la part de l'employé et présenté comme preuve, notamment, une liste de courriels écrits et envoyés par l'employé. L'employé avait demandé que ces documents spécifiques soient retirés des procédures dans la mesure où aucune autorisation préalable de la CNPD n'avait été obtenue. (N.B. : dans le droit luxembourgeois, la surveillance de la correspondance électronique d'un employé doit faire l'objet d'une autorisation préalable de la CNPD).

Après avoir établi qu'aucune autorisation préalable n'avait été octroyée dans ce cas et avoir évoqué les droits fondamentaux du secret de la correspondance, ainsi que le droit au respect de la vie privée, le tribunal de première instance a établi que lesdits documents devaient être retirés des procédures.

Cette décision est très intéressante, au sens où le tribunal de première instance, dans le domaine de la surveillance des courriels, a pris l'exact contrepied de la majorité des jugements prononcés dans le domaine de la vidéosurveillance, où la plupart des décisions établissent que les images peuvent être admises en tant que preuves même en l'absence d'autorisation préalable de la CNPD. Il convient néanmoins de noter qu'il ne s'agissait que d'un jugement en première instance et que la société X peut avoir fait appel. Aucune décision n'avait toutefois été publiée au jour de la rédaction des présentes.

C. Autres informations importantes

En 2013, la première association pour le respect de la vie privée et la protection des données a été établie au Luxembourg. Les membres de l'APDL (Association pour la protection des données au Luxembourg) sont principalement des délégués à la protection des données, des experts en sécurité informatique et des délégués à la conformité, ainsi que des avocats et des consultants.

MALTE

A : Résumé des activités et actualités

En 2013, le bureau du commissaire à la protection des données et de l'information a maintenu une approche proactive pour rencontrer les secteurs dans le ferme objectif de discuter de leurs opérations commerciales et de résoudre tout problème de protection des données susceptible de requérir une intervention du commissaire. Le bureau adopte une approche qui permet de coordonner ces rencontres avec la vaste représentation des secteurs respectifs. Cette approche a prouvé son efficacité en donnant des résultats satisfaisants, particulièrement lorsque les lignes directrices ou les codes de bonnes pratiques auraient besoin d'être développés pour réglementer des domaines spécifiques du secteur.

Bien qu'aucune intervention législative n'ait concerné la loi sur la protection des données ou la législation subsidiaire y afférente, le bureau a réalisé, au cours de l'année, des exercices d'examen interne conçus pour mettre en œuvre la politique globale du gouvernement et assurer une meilleure réglementation.

En mars, les électeurs ont été appelés aux urnes afin d'exprimer leurs préférences dans le cadre d'élections générales. Pendant la campagne électorale, le bureau a vu le nombre de plaintes reçues augmenter de manière considérable. La plupart ont été déposées par des personnes concernées qui s'opposaient à une violation de leurs droits à la protection des données par des partis politiques ou des candidats aux élections qui leur avaient envoyé des messages électoraux par voie électronique ou SMS. Les plaintes ont été déposées par des personnes n'appartenant à aucun parti et n'ayant pas préalablement consenti à recevoir ce type de messages non sollicités.

Face à cette situation, le commissaire a convoqué une réunion des principaux partis politiques immédiatement après les élections afin de les informer que le temps était venu de développer des lignes directrices sur le traitement des données à caractère personnel pour les campagnes électorales. Ces lignes directrices ont pour objet de fournir une interprétation claire et uniforme de l'applicabilité de la loi sur la protection des données dans un environnement politique où les candidats et les partis politiques traitent des données à caractère personnel concernant des personnes aux fins de leurs campagnes électorales et de la promotion de leur idéologie politique. Suite à une série de réunions et de contributions écrites reçues de la part des partis concernés, le bureau a préparé une version finale qui devra faire l'objet d'un accord et, en termes de calendrier établi, devrait être adoptée au troisième trimestre de 2014.

Pendant la période examinée, le bureau a continué d'honorer ses engagements européens et internationaux en participant à plusieurs forums sur la protection des données. Le 28 janvier, comme les années précédentes, le bureau a préparé de la documentation informative et des articles de papeterie qui ont été distribués aux élèves de niveaux prédéterminés, dont le concept et le message inhérent étaient la sécurité sur Internet.

Concernant la mise en œuvre de la loi sur la liberté d'information, les autorités publiques ont acquis de l'expérience en 2013 grâce à la mise en œuvre de la loi et au traitement des demandes de documentation via le système informatique ad hoc. L'intervention et l'aide apportée par l'unité de coordination de la liberté d'information, établie au sein du ministère de tutelle du bureau, ont aidé les autorités publiques à atteindre ces objectifs.

Au total, les autorités publiques ont géré 130 demandes d'informations, dont 10 reportées de 2012. Sur ce total, 71 (54,6 %) ont été acceptées et 51 (39,2 %) ont été rejetées. Le nombre de demandes toujours en attente d'une décision en fin d'année était de 4 (3,1 %). 4 autres demandes (3,1 %) ont été abandonnées par leurs auteurs. Sur les demandes rejetées, 14 (27,4 %) portaient sur l'examen d'une décision par le commissaire. Le commissaire a accepté dans un cas et rejeté les 13 autres. Sur ces 13 cas, 3 ont fait appel devant la cour d'appel pour la protection des données et de l'information. Une

quatrième personne s'est sentie lésée par une décision du commissaire en matière de protection des données et a fait appel devant la cour d'appel.

En fin d'année, l'ensemble de ces appels attendaient encore un jugement et le recrutement de nouveaux membres de la Cour après que les anciens membres avaient donné leur démission suite au changement d'administration publique.

Organisation	Bureau du commissaire à la protection des données et de l'information
Président et/ou collège	Commissaire à la protection des données et de l'information
Budget	Env. 280 000 €
Personnel	Commissaire – 1 Personnel spécialisé – 3 Assistance technique – 2 Assistance administrative – 3
Activités générales	
Décisions, avis, recommandations	Le commissaire a émis 81 décisions sur la protection des données et la liberté d'information. 28 avis/recommandations concernant des sujets spécifiques à la protection des données ont été émis par le commissaire et adressés aux responsables du traitement des données.
Notifications	240 nouveaux formulaires de notification
Contrôles préalables	6 demandes de contrôles préalables ont été reçues
Demandes émanant de personnes concernées	Les demandes par téléphone représentent en moyenne 10 appels par jour, tandis que les demandes par courriel s'élèvent à environ 250
Plaintes émanant de personnes concernées	144 plaintes sur la protection des données et 14 sur la liberté d'information.
Conseils sollicités par le Parlement ou le gouvernement	1 demande du ministère de l'éducation et de l'emploi avait trait à la rédaction d'un instrument juridique demandant les données à caractère personnel des étudiants afin de développer des politiques visant à résoudre le problème croissant des élèves ayant des notes insuffisantes.
Autres renseignements relatifs aux activités générales	S. o.
Activités d'inspection	

Contrôles, enquêtes	10 contrôles sur place ont été réalisés principalement dans le cadre de procédures d'enquêtes suite à des plaintes.
Activités de sanction	
Sanctions	Des avertissements officiels ont été adressés à des responsables du traitement des données, mais aucune procédure judiciaire n'a été ouverte devant les tribunaux.
Amendes	1 amende a été imposée à un responsable du traitement des données suite à un délit répété établi après la conclusion d'une enquête.
DPD	
Chiffres relatifs aux DPD	14 représentants des données à caractère personnel 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 à caractère personnel. En général, la DPA néerlandaise se focalise sur une 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 signalements que nous recevons de la part de différentes sources de la société via divers canaux, tels que des appels téléphoniques, des courriels, des articles de presse, etc. En 2011, un nouveau système d'enregistrement des signalements a été introduit, qui permet à la DPA néerlandaise d'enregistrer les signalements par secteur. L'évaluation des risques tient compte de la gravité de l'infraction présumée, du nombre de personnes touchées, de la clarté de l'indication de la violation, et de la faisabilité légale d'une mesure d'application, ainsi que des répercussions de l'utilisation de nouvelles technologies à grande échelle.

En 2013, la DPA néerlandaise s'est essentiellement focalisée sur les éléments suivants : le profilage, la protection adéquate des données médicales et le traitement de données dans le cadre des relations de travail. Les activités déployées par la DPA néerlandaise en 2013 se sont en outre focalisées, notamment, sur les principes de limitation de la finalité, de consentement, de transparence et de sécurité des données.

L'une des principales enquêtes réalisées en 2013 portait sur la protection des données médicales. Tout le monde a droit au même niveau de protection contre des accès non autorisés à ses données médicales. Une enquête menée par la DPA néerlandaise auprès de différents établissements de santé, cliniques de garde et pharmaciens a néanmoins démontré que les mesures de sécurité prises pour protéger les données des patients contre ces accès non autorisés présentaient de nombreux problèmes. Des mesures de sécurité insuffisantes présentent le risque que des employés aucunement concernés par le traitement du patient puissent quand même accéder à son dossier médical. La DPA néerlandaise considère, sur la base des enquêtes réalisées, des signalements reçus et de conversations avec les organisations professionnelles, que les problèmes détectés semblent relativement courants dans le secteur de la santé.

Le transfert des données de patient par un prestataire de soins à un autre, par exemple du cabinet d'un médecin à une compagnie d'assurance ou pharmaceutique, fait l'objet de garanties très strictes. Ces transferts ne sont pas autorisés sans le consentement de la personne concernée. La DPA néerlandaise a enquêté sur le transfert de données médicales par des pharmaciens au profit d'une entreprise de produits destinés aux personnes souffrant d'incontinence, et a conclu que les pharmaciens n'avaient pas pris suffisamment de précautions pour protéger les données des patients. Par ailleurs, tous les patients n'avaient pas donné leur consentement au transfert de leurs données à la société pharmaceutique.

D'autres enquêtes réalisées en 2013 ont porté sur les données en ligne et le profilage. Les données sur les programmes de télévision regardés, sur les sites web visités et sur les applications téléchargées en disent long sur le comportement et les préférences d'une personne, mais il n'est pas souvent clair de ce qu'il advient de ces données collectées par les opérateurs de télécommunications et développeurs d'applications. La plupart des gens n'ont pas conscience du fait que, en réalité, ils paient ces services dits « gratuits » avec leurs données à caractère personnel. Les sociétés et entreprises doivent fournir suffisamment d'informations aux personnes sur l'utilisation de leurs données et leur demander leur consentement lorsque nécessaire.

L'une des enquêtes réalisées à ce sujet en 2013 a porté sur les analyses illégitimes de données (inspections de paquets) entreprises par quatre opérateurs de télécommunications. Il en est ressorti que

ces entreprises stockaient des données sur les sites web et les applications visités par leurs clients, en violation de la loi et ce, sans en informer correctement leurs clients.

Des questions parlementaires sur l'utilisation de cookies par la télévision publique néerlandaise (Nederlandse Publieke Omroep – NPO) sur ses sites web ont amené la DPA néerlandaise à émettre de nouveaux conseils sur le cadre juridique à cet égard et à déclarer que la NPO n'était pas autorisée à refuser aux visiteurs l'accès à son site web s'ils ne consentaient pas à ce que leur comportement de navigation soit pisté.

Outre ces enquêtes, la DPA néerlandaise conseille le gouvernement sur les projets de loi avant qu'ils ne soient envoyés au Parlement. Grâce à ses conseils, des propositions sont (parfois) amendées afin d'éviter des violations de la vie privée.

En 2013, des conseils ont été donnés sur le projet de loi relative à la jeunesse (Jeugdwet). Le projet de loi relative à la jeunesse traite de la délégation des tâches tant administratives que financières, du gouvernement national aux municipalités en ce qui concerne l'assistance, l'aide et les soins liés à l'éducation des enfants et des jeunes souffrant de troubles psychologiques. La division exacte des tâches n'est pas encore totalement claire, mais la DPA néerlandaise s'attend à ce que la décentralisation, une tendance qu'elle a plus souvent détectée dans le cadre d'autres propositions législatives, entraîne une augmentation des quantités de données traitées par les municipalités. L'approche exhaustive des problèmes de la jeunesse et de la famille devrait en outre accroître l'échange d'informations entre les différents acteurs, ainsi que les risques d'opérations de traitement de données excessives, d'utilisations (illicites) de données à d'autres fins (non compatibles) et de mesures de sécurité insuffisantes.

D'après les informations publiques disponibles sur la décentralisation du système d'aide à la jeunesse, il semblerait que les municipalités et autres parties concernées ne prennent pas les mesures adéquates pour réduire ces risques. Le projet de loi ne semble pas non plus prévoir les ressources nécessaires pour développer un système qui assure la minutie et la légitimité du traitement des données. La DPA néerlandaise estime par conséquent que les municipalités devraient être obligées de réaliser des évaluations de l'impact sur la vie privée et des audits sur les opérations (actuelles et proposées) de traitement de données. Cette approche devrait être prévue dans la loi sur la jeunesse proposée ou une législation secondaire.

Organisation	Autorité néerlandaise de protection des données
Président et/ou collège	Jacob Kohnstamm – Président Wilbert Tomesen – Commissaire et vice-président Madeleine McLaggan-Van Roon – Commissaire* *Mme McLaggan a été exemptée de ses tâches de commissaire de la DPA néerlandaise le temps de préparer un rapport scientifique sur les relations entre la loi sur la concurrence et la protection des données à la demande du secrétaire d'État à la sécurité et la justice.*
Budget	Alloué : 7 586 000 € Exécuté : 7 827 000 €
Personnel	74,9 ETP
Activités générales	

Décisions, avis, recommandations	109 (lignes directrices, avis, codes de conduite, affaires internationales, exemptions, sanctions et transferts internationaux)
Notifications	3 523
Contrôles préalables	86
Signalements ([6]) émanant de personnes concernées	6 879
Conseils sollicités par le Parlement ou le gouvernement	30
Autres renseignements relatifs aux activités générales	S. o.
Activités d'inspection	
Contrôles, enquêtes	73
Activités de sanction	
Sanctions	19
Amendes	S. o.
DPD	
Chiffres relatifs aux DPD	369 (dans 362 organisations)

B. Informations sur la jurisprudence

Pendant l'année sur laquelle porte ce rapport, plusieurs affaires liées à la protection des données ont été traitées par les tribunaux néerlandais. L'une des affaires concernait une plaignante qui avait demandé à l'institut médico-légal national s'il était possible d'utiliser une goutte de sang d'une personne décédée, que l'institut conservait dans l'un de ses fichiers, afin de déterminer si elles avaient un lien familial. Suite aux objections des filles de la personne décédée, l'utilisation de cette goutte de sang a été refusée. La plaignante a fait appel de cette décision devant le parquet et l'institut, ce à quoi le parquet a répondu que la décision de ne pas autoriser l'utilisation de sang ne pouvait être considérée comme une décision ayant des effets juridiques aux termes de la loi sur les données judiciaires et le casier judiciaire, et que son appel n'était par conséquent pas admissible.

La plaignante a fait appel de cette réponse devant le tribunal de Rotterdam, qui a examiné si cette décision était bien une décision n'ayant aucun effet juridique aux termes de la loi sur les données judiciaires et le casier judiciaire. Le tribunal a conclu que ni la loi sur les données judiciaires et le casier judiciaire ni la loi sur les entreprises n'étaient applicables dans cette situation. Étant donné l'implication de matériel biologique, la loi applicable était la loi néerlandaise sur la protection des données. La plaignante aurait par conséquent dû s'adresser à un tribunal civil et interjeter appel sur la base de la loi

[6] Depuis avril 2011, tous les contacts des citoyens sont enregistrés sous forme de signalements. Ces signalements servent à classer nos interventions par ordre de priorité. Ces signalements ne sont donc pas mesurés en fonction de la manière dont ils sont reçus par la DPA, mais du secteur dont ils dépendent.

sur la protection des données plutôt qu'auprès du parquet et de l'institut médico-légal national dans le cadre d'une procédure administrative.

Dans le cadre d'une autre affaire en 2013, un plaignant a interjeté appel devant la Cour administrative suprême alléguant que le droit d'accès, de rectification ou de suppression d'informations contenues dans un fichier des services de l'immigration et des naturalisations néerlandais (IND) le concernant lui avait été illégitimement refusé.

Le plaignant était en possession d'un permis de résidence sur la base de son mariage avec la personne X. Le ministre de la justice a alors reçu une lettre anonyme affirmant que le plaignant n'était pas l'époux de la personne X mais qu'ils étaient frère et sœur. Le ministre a alors adressé un courrier au plaignant déclarant que, suite à des informations reçues anonymement, le ministre avait l'intention de refuser le permis de résidence du plaignant, auquel il offrait la possibilité d'une coopération volontaire pour la réalisation d'un test ADN afin d'établir les faits. Le plaignant a refusé le test ADN. Suite à ce refus, il est devenu techniquement impossible de déterminer si la lettre anonyme établissait des faits et le ministre a dû décider de ne pas annuler le permis de résidence.

Le plaignant a ensuite exprimé sa volonté de poursuivre l'auteur de la lettre anonyme pour diffamation et demandé à avoir accès à ce document à des fins de rectification ou de suppression. Le plaignant estimait en effet que, la lettre contenant des informations personnelles le concernant, il devait pouvoir y avoir accès et être autorisé à la détruire. Le ministre lui a refusé cet accès, arguant qu'il était nécessaire de protéger une autre personne et les droits et libertés des autres. Par ailleurs, le plaignant a eu un aperçu factuel du contenu de la lettre. Le tribunal a confirmé et ajouté que le contenu de la lettre ne concernait pas des données à caractère personnel du plaignant. Le plaignant a interjeté appel devant la Cour administrative suprême sur la base de l'article 8 de la Convention européenne des droits de l'homme (CEDH).

La Cour administrative suprême a jugé que le droit de correction prévu dans la loi néerlandaise sur la protection des données n'a pas vocation à autoriser la rectification ou la suppression d'informations qui ne plaisent pas au plaignant. Le fait que les informations figurant dans la lettre en question soient correctes ou non, devrait être évalué dans le cadre d'une procédure appropriée. Cette procédure d'enquête portant sur le permis de résidence du plaignant a été déployée. Le fait que l'enquête ait conclu à l'impossibilité technique d'établir les faits n'a aucune influence sur le fait que le ministre juge la lettre pertinente et qu'il a le droit de la conserver après avoir pris en compte ses intérêts par rapport à ceux du plaignant vis-à-vis de la destruction de la lettre. Il a par ailleurs été établi que la protection du demandeur avait été correctement jugée plus importante que les intérêts du plaignant. La décision de ne pas supprimer la lettre, dans la mesure où il se serait agi d'une violation de ses droits en vertu de l'article 8 de la CEDH, est par conséquent validée par la loi néerlandaise sur la protection des données comme par l'article 8, paragraphe 2, de la CEDH.

POLOGNE

A. Résumé des activités et actualités

Au 22 mars 2013, l'inspecteur général pour la protection des données à caractère personnel (GIODO) est devenu l'autorité compétente pour accepter les notifications de violations de données à caractère personnel faites par des fournisseurs de services de télécommunications accessibles au public. Cette nouvelle obligation est une conséquence de la modification de la loi sur les télécommunications, qui met en œuvre, dans le droit polonais, les dispositions de la directive 2002/58/CE vie privée et communications électroniques, introduites par la directive 2009/136/CE du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel, ou directive sur les droits des citoyens.

Concernant l'obligation ci-dessus, un formulaire électronique adéquat a été développé pour signaler des violations de la protection des données, et une équipe dédiée aux violations de données a été créée pour analyser les violations de données, notamment en évaluant l'adéquation des recours introduits par les opérateurs vis-à-vis des violations signalées.

En 2013, le GIODO a reçu 139 notifications de violations de données de la part d'opérateurs de télécommunications.

En 2013, le GIODO a régulièrement modifié et amélioré les moyens de communications électroniques avec les responsables du traitement des données et les citoyens. Des activités ont également été déployées dans le cadre de la migration des technologies informatiques appliquées d'une architecture client-serveur vers une technologie utilisant une architecture de nuage privé.

Le GIODO a poursuivi sa participation aux travaux liés à la réforme du cadre de la protection des données dans l'UE. Parmi les événements les plus importants à cet égard, il convient de citer les suivants :

1. Le 1er mars 2013, l'inspecteur général a rencontré Françoise Le Bail, directrice générale de la DG Justice de la Commission européenne. Cette réunion était consacrée à l'analyse des progrès de la réforme du cadre de protection des données de l'UE et les participants ont évoqué les sujets les plus controversés dans le débat en cours ou les plus importants pour la future orientation des dispositions sur la protection des données à caractère personnel en Europe.

2. Le 16 avril 2013, une réunion conjointe des comités du Sénat a été organisée au Sénat (la chambre supérieure du Parlement polonais) en coopération avec le GIODO. Pendant ce débat, les principales orientations des changements du cadre de protection des données de l'UE, l'impact du règlement général sur la situation des entrepreneurs et des consommateurs polonais, et sa relation aux dispositions nationales à la lumière des défis de la mondialisation et des modèles commerciaux contemporains, ont également été évoqués.

3. Le 4 avril 2013, le GIODO, ainsi que des représentants de la CE, la représentation permanente de la République de Pologne auprès de l'UE, des députés européens, des représentants de ministères, des ONG, des entreprises, des universitaires et des experts indépendants ont participé à une discussion sur la réforme de la protection des données organisée par le ministère de l'administration et de la numérisation, l'une des principales autorités sur les travaux sur le règlement général en Pologne. Une réunion similaire dédiée à la réforme s'est tenue le 13 mai 2013 dans le cadre du débat « identité numérique : Qui sommes-nous en ligne et de quelle manière partageons-nous les informations sur nous-mêmes ? ». La commissaire Viviane Reding, vice-présidente de la Commission européenne, qui dirige les travaux sur la proposition du nouveau règlement du Parlement européen et du Conseil de l'Union européenne, était une invitée spéciale de cette dernière réunion.

Organisation	Bureau de l'inspecteur général pour la protection des données à caractère personnel (GIODO)
Président et/ou collège	Dr Wojciech Rafał Wiewiórowski, inspecteur général pour la protection des données à caractère personnel
Budget	15 060 000 PLN
Personnel	135 employés.
Activités générales	
Décisions, avis, recommandations	1 358 décisions émises (504 décisions liées aux procédures d'enregistrement, 74 en relation avec des enquêtes réalisées, 646 en conséquence de procédures ouvertes par une plainte, 134 concernant l'autorisation de transfert de données vers un pays tiers et 109 liées à une exécution administrative). 121 demandes ont été adressées à des autorités publiques, des autorités des territoires autonomes, ainsi qu'à des unités organisationnelles nationales et municipales, des entités privées exécutant des tâches publiques, des personnes physiques et morales, des unités organisationnelles sans personnalité juridique et d'autres entités, afin d'assurer une protection efficace des données à caractère personnel.
Notifications	16 866 fichiers de données à caractère personnel enregistrés.
Contrôles préalables	En conséquence des procédures d'enregistrement (contrôles préalables), 2 279 fichiers de données à caractère personnel contenant des données sensibles ont été inscrits au registre correspondant ; le traitement de fichiers de données à caractère personnel contenant des données sensibles ne peut commencer qu'une fois la procédure d'enregistrement terminée.
Demandes émanant de personnes concernées	4 911 questions juridiques ont été envoyées à la DPA polonaise. 11 908 explications ont également été fournies grâce à la ligne d'information du GIODO.
Plaintes émanant de personnes concernées	Plaintes concernant des atteintes à la protection des données à caractère personnel, notamment dans les domaines suivants : - l'administration publique (126 plaintes), - les tribunaux, les services du procureur général, la police, les huissiers (56 plaintes), - les banques et autres établissements financiers (127 plaintes), - Internet (124 plaintes), - le marketing (31 plaintes), - les questions liées au logement (57 plaintes), - les assurances sociales, de biens et individuelles (50

	plaintes), - les organismes sociaux (12 plaintes), - les télécommunications (24 plaintes), - l'emploi (11 plaintes), - le recouvrement de créances (42 plaintes), - l'éducation (21 plaintes) - la santé (34 plaintes), - autres (386 plaintes).
Conseils sollicités par le Parlement ou le gouvernement	Des avis ont été exprimés sur 617 projets de lois soumis à l'examen du GIODO.
Autres renseignements relatifs aux activités générales	60 formations ont été assurées par le GIODO sur les dispositions relatives à la protection des données à caractère personnel, surtout au bénéfice d'institutions publiques. 209 établissements scolaires, dont des écoles primaires, élémentaires et secondaires, et centres de formation professionnelle destinés aux enseignants, ont participé à la 4e édition du programme, déployé dans toute la Pologne, appelé « Vos données, votre préoccupation : une initiative éducative destinée aux élèves et aux enseignants » pour l'année scolaire 2013/2014.
Activités d'inspection	
Contrôles, enquêtes	173 contrôles ont été réalisés en 2013. Contrôles sectoriels sur : - des services en ligne (y compris les boutiques en ligne) – 10 contrôles, - des entités développant des programmes de fidélisation – 7 contrôles, - des grandes enseignes faisant appel à des applications RFID – 8 contrôles, - des autorités territoriales autonomes qui collectent des données à des fins de ramassage des ordures (en lien avec l'exécution de la loi sur la propreté) – 15 contrôles, - des unités de police utilisant le système « e-posterunek » (poste de police électronique facilitant le travail de la police) – 8 contrôles, - des autorités autorisées à traiter des données dans le système d'information national et le système d'information sur les visas – 14 contrôles, - - des fournisseurs de services de télécommunications (en lien avec des incidents de violations de données) – 14 contrôles.
Activités de sanction	

Sanctions	Le GIODO ne tient pas de statistiques générales sur les sanctions. Toutefois, vis-à-vis des pouvoirs conférés au GIODO en tant qu'autorité d'application, par exemple, 109 procédures administratives ont été instituées dans le cadre de l'exécution des décisions du GIODO. En ce qui concerne les contrôles réalisés en 2013, le GIODO a ouvert des procédures administratives à l'encontre de responsables du traitement des données et prononcé 74 décisions administratives dont un arrêté ordonnant la restauration d'un état de droit approprié. Le GIODO a également émis 92 décisions de refus d'enregistrer un fichier de données. La DPA n'a imposé aucune sanction pendant la période de référence.
Amendes	Aucune amende n'a été imposée en 2013.
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

En 2013, 52 décisions administratives sur 646 émises par le GIODO ont fait l'objet d'un appel devant le tribunal administratif de Voïévodie à Varsovie. En comparaison, en 2012, 70 décisions avaient fait l'objet d'un appel, ce qui représente 18 de moins en 2013.

Parmi les jugements rendus suite à des plaintes d'entités contre les décisions de la DPA, il convient de souligner celui de la Cour administrative suprême du 21 août 2013 (réf. nº I OSK 166/12). Dans ce jugement, la Cour a indiqué que l'article 18(6) de la loi sur la prestation de services par voie électronique imposait uniquement l'obligation de fournir des informations sur des données aux autorités publiques aux fins de la conduite des procédures, tandis qu'il n'existe aucune obligation de divulguer ces données aux personnes dont les droits ont été violés. Les autorités ordonnant la divulgation des données et la cour administrative examinant la plainte contre cette décision doivent systématiquement prendre en compte les circonstances individuelles de chaque affaire et trouver un juste équilibre entre des intérêts opposés, c.-à-d. le droit à la protection des données à caractère personnel d'un côté et, de l'autre, le droit à la dignité, la réputation, ou l'image de marque d'une entreprise. Ce faisant, les exigences découlant du principe de proportionnalité doivent être bien prises en compte, de manière à ce que les mesures appliquées soient adaptées au risque pesant sur l'intérêt requérant une protection supérieure dans un cas spécifique. La Cour administrative suprême a souligné que les circonstances juridiques actuelles permettent de conclure que, en vertu du droit en vigueur, il est possible de demander la divulgation de données collectées par le responsable du traitement d'un service en ligne en se basant sur une loi moins restrictive que la loi sur la prestation de services par voie électronique, à savoir la loi sur la protection des données à caractère personnel et, plus spécifiquement, son article 23 (traitement de données, y compris leur divulgation), mais sous réserve de certaines conditions. Ce dernier article prévoit la proportionnalité des moyens et des finalités, ainsi que l'équilibre de la protection des différents intérêts : liberté d'expression et droit à la protection des intérêts personnels. L'entité demandant la divulgation de données à caractère personnel doit justifier son point de vue. En vertu de l'article 23 (1) (5), il doit s'agir « d'intérêts légitimes ». En cas de refus de divulguer les données par l'entité, la partie responsable du traitement peut soumettre une demande au GIODO, qui peut ordonner la divulgation des données à caractère personnel par le biais d'une décision après avoir suivi les procédures pertinentes. À cet égard,

l'évaluation du GIODO est importante et doit dépendre des circonstances d'un cas donné, dans la mesure où la loi sur la prestation de services par voie électronique et la loi sur la protection des données à caractère personnel seront alors applicables. Lorsqu'il prend une décision, le GIODO doit évaluer dans chaque cas quels intérêts protégés par la loi sont les plus importants, les données à caractère personnel ou les intérêts économiques de la société.

En 2013, la Cour administrative suprême a rejeté en dernière instance l'appel d'un maire contre un jugement du tribunal administratif de Voïévodie du 24 novembre 2011 (réf. nº II SA/Wa 1828/11). Dans son jugement du 14 mars 2013 (réf. nº I OSK 620/12), la Cour administrative suprême a rappelé la validité des décisions du GIODO dans ses procédures administratives. Dans son jugement susmentionné, la Cour administrative suprême a souligné ce qui suit : « En examinant la légitimité du traitement de données à caractère personnel (...) le GIODO et le tribunal de première instance ont appliqué de manière approprié les principes spécifiant l'admissibilité du traitement de données à caractère personnel prévue à l'article 23(1) de la loi, en supposant que les conditions préalables qui légitiment le traitement de ces données soient celles qui sont énumérées au point 2 de la disposition ci-dessus. Ce dernier autorise le traitement de données à caractère personnel s'il est nécessaire aux fins de l'exercice des droits et devoirs résultant d'une disposition juridique. Dans ce cas, l'obligation découlant d'une disposition juridique portant sur le maire, en ce qui concerne le contenu de la résolution du conseil municipal dans sa publication officielle en ligne (bulletin d'information public, BIP), pourrait être de respecter cette obligation sans divulguer les données à caractère personnel du plaignant. Si la publication d'informations dans le BIP répond à des fins de transparence de l'activité publique du conseil municipal, y compris le contenu de ses résolutions, alors ces mêmes fins peuvent être atteintes lorsque les données de personnes physiques sont effacées des informations, afin de protéger leur vie privée.

C. Autres informations importantes

Sur la période de référence, le nombre de fichiers notifiés à des fins d'enregistrement a augmenté (**de 40 % par rapport à 2012, de 81 % par rapport à 2011 et de 242 % par rapport à 2010**). Il convient par ailleurs de noter que le nombre de notifications émanant d'entités privées augmente de plus en plus : de 95 % en 2013 par rapport à 2012, tandis que le nombre de notifications émanant d'entités publique sur cette période a augmenté de 3 %. Par conséquent, sur la période de référence, jusqu'à 46 % du nombre total de fichiers notifiés émanaient d'entités privées, alors qu'en 2012 et 2011, ce taux s'élevait à 31-32 %. En 2013, le GIODO a traité **3 709** notifications de mise à jour soumises par des responsables du traitement des données, et émis 340 décisions de suppression de fichiers de données du registre polonais des fichiers de données à caractère personnel.

À l'occasion de la journée européenne de la protection des données, le 28 janvier 2013, l'inspecteur général a organisé une traditionnelle journée portes ouvertes pour tous les citoyens, ainsi qu'une conférence intitulée « Protection des données à caractère personnel dans la santé et les essais cliniques ». Comme à l'habitude, la journée européenne de la protection des données a également été célébrée à Bruxelles. Le GIODO a également activement participé à la 5e conférence internationale sur les ordinateurs, le respect de la vie privée et la protection des données (23-25 janvier), dans le cadre de laquelle, le 23 janvier 2013, un panel spécial intitulé « *de la 'Solidarité' à une société de surveillance. Dilemmes liés à la protection de la vie privée en Pologne* » a été organisé par la DPA polonaise pour évoquer la législation polonaise.

Le GIODO a poursuivi son initiative qui consiste à organiser d'autres journées portes ouvertes dans d'autres villes polonaises, et organisé la 3e journée portes ouvertes les 6 et 7 mai 2013 à Poznań, qui a accueilli, notamment, une conférence scientifique sur les aspects juridiques et économiques du traitement de données à caractère personnel à des fins économiques, ainsi qu'une série de réunions sous forme de séminaires et de formations s'adressant à l'administration publique.

Les 23 et 26 septembre 2013, le GIODO a accueilli la 35e Conférence internationale des commissaires à la protection des données et de la vie privée, « Vie privée : Une boussole dans un monde incertain » à

Varsovie, en Pologne. La conférence a permis de mieux comprendre les questions de protection des données à travers le monde, et de définir les motifs de l'échange des expériences et des avis dans ce domaine. Elle a également donné une meilleure explication des problèmes liés à la protection des données. Lors de la session fermée de la 35e conférence internationale, nous avons accueilli 66 délégations du monde entier. L'expérience et les connaissances d'un si grand nombre de participants ont offert une possibilité unique d'adopter 8 résolutions concernant différents domaines de la protection des données : l'accréditation, le profilage, l'orientation stratégique de la conférence, la coordination de l'application sur le plan international, la transparence des pratiques liées aux données à caractère personnel, l'éducation numérique pour tous, le pistage sur Internet et la protection de la vie privée. La « déclaration de Varsovie sur "l'applification" de la société » a par ailleurs été adoptée. La conférence ouverte a rassemblé des représentants de nombreux milieux, notamment politique, scientifique, commercial, ONG nationales et internationales, qui ont débattu en groupes sur trois thèmes distincts : « Les réformes à travers le monde. Interopérabilité entre les régions », « Vie privée et technologies », et « Acteurs : perspectives, rôles, intérêts ». À l'occasion de la conférence ouverte, la « déclaration de Varsovie 2013 : un appel à mesures d'incitation afin de promouvoir la désignation de délégués à la protection des données » a été adopté par la confédération européenne des organisations de protection des données et les associations nationales de DPD en Europe.

En 2013, le **projet PHAEDRA** (*Improving practical and helpful cooperation between data protection authorities*), cofinancé par la Commission européenne en vertu des subventions à l'action du programme « Droits fondamentaux et citoyenneté », a été lancé. Le GIODO participe au projet en tant que membre du consortium de projet. Le projet est réalisé en coopération avec Vrije Universiteit Brussel (coordinateur du projet), UK Trilateral Research & Consulting LLP (partenaire) et l'université espagnole Jaume I (partenaire). L'objectif de base du projet est d'identifier les problèmes qui freinent la coopération entre certaines autorités de protection des données et d'autres entités publiques traitant ce problème, et de présenter des recommandations visant à améliorer la situation. Le projet a par conséquent vocation à contribuer à améliorer la coopération et la coordination entre l'ensemble des parties intéressées. Le projet doit être finalisé en 2015.

PORTUGAL

A. Résumé des activités et actualités

En mai 2013, la DPA portugaise a accueilli la conférence de printemps sur la protection des données, qui s'est tenue à Lisbonne en présence d'environ 130 participants afin de discuter du thème de la *Protection de la vie privée : les futurs défis*. Au beau milieu de la réforme de la protection des données et pendant la modernisation de la Convention 108, la conférence des commissaires européens a discuté de questions importantes pour l'avenir de la protection des données, telles que le concept de données à caractère personnel, les droits des personnes concernées sur Internet, la sécurité des informations en tant que priorité, le renforcement de la supervision et la coopération.

La DPA portugaise a signé un protocole de coopération avec le centre de recherche de la faculté de droit de l'université de Lisbonne afin de sensibiliser conjointement aux questions de la protection des données et de la vie privée, et de s'entraider sur des initiatives communes.

La DPA a émis de nouveaux conseils sur le contrôle de l'utilisation des TIC dans le contexte de l'emploi, en révisant ses lignes directrices de 2002 et en tenant compte de la nouvelle législation du travail et des développements observés dans ce domaine, ce qui a rendu nécessaire de mettre à jour et de détailler certains aspects de l'utilisation privée des TIC par les employés http://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf

La DPA a également fait suite au développement du projet de dossiers médicaux électroniques en autorisant la phase II de la plateforme de dossiers médicaux (PDS), en imposant des conditions importantes au traitement de données à caractère personnel et en incluant la mise en œuvre d'outils de prise en compte du respect de la vie privée dès la conception, afin d'améliorer le respect de la vie privée des citoyens tout en leur octroyant le contrôle de l'accès et de l'utilisation de leurs données.

Suite à la mise en œuvre pratique de la mise à jour de la directive vie privée et communications électroniques, la DPA portugaise a rencontré des représentants des acteurs économiques du secteur du marketing et du commerce en ligne, afin de discuter du nouveau cadre juridique en ce qui concerne, notamment, les cookies.

Concernant les notifications électroniques, la DPA a développé des formulaires de notification plus spécifiques pour les cas particuliers, pour le traitement des données de vidéosurveillance, augmentant ainsi le nombre de procédures entièrement électroniques.

Organisation	CNPD – Comissão Nacional de Protecção de Dados
Président et/ou collège	Prof. Filipa Calvão (présidente)
Budget	2 356 436 euros
Personnel	De 25 à **18** (d'ici la fin de l'année) en raison de restrictions légales imposées aux services publics
Activités générales	
Décisions, avis, recommandations	12 285
Notifications	11 170
Contrôles préalables	10 280

Demandes émanant de personnes concernées	89 demandes concernant l'exercice du droit d'accès et de suppression du Système d'information Schengen
Plaintes émanant de personnes concernées	652
Conseils sollicités par le Parlement ou le gouvernement	88
Autres renseignements relatifs aux activités générales	259 demandes d'accès à des données à caractère personnel par des tierces parties 910 demandes d'avis sur la levée de la confidentialité de l'appelant en raison d'appels téléphoniques dérangeants 2 585 demandes d'informations (de la part de responsables du traitement des données et de personnes concernées) envoyées par écrit via le site web du bureau
Activités d'inspection	
Contrôles, enquêtes	246
Activités de sanction	
Sanctions	158
Amendes	± 205 000 EUR
DPD	
Chiffres relatifs aux DPD	Sans objet

RÉPUBLIQUE TCHÈQUE

A. Résumé des activités et actualités

Les activités de contrôle se concentrent sur le programme d'inspection du bureau et les plaintes des citoyens. Plusieurs cas ont été sélectionnés et décrits ci-dessous. Les domaines où des contrôles ont été prévus sont les suivants : Traitement de données à caractère personnel dans le Système d'information Schengen national, traitement de données concernant des bénéficiaires de dons (tels que des fonds du FSE), gestion de données par des organismes de l'administration publique, traitement de données à caractère personnel dans le secteur des services et du commerce.

Les 11 et 12 février 2013, nous avons accueilli une **visite d'étude** de la DPA moldave. L'événement a été financé et a bénéficié de l'aide logistique du programme TAIEX. Question abordée : Protection des données à caractère personnel dans les médias de la presse écrite et audio-visuelle.

Les 21 et 22 mai 2013, nous avons accueilli une **visite d'étude** de la DPA de l'ancienne République yougoslave de Macédoine, financée par le TAIEX. L'événement a été financé et a bénéficié de l'aide logistique du programme TAIEX. Question abordée : Protection des données dans le Système d'information Schengen.

Deux de nos experts ont par ailleurs participé en tant qu'orateurs à des ateliers du TAIEX en Moldavie et en Bosnie-Herzégovine.

Les 15 et 16 avril 2013, la **53e réunion** du groupe de travail international sur la protection des données dans les télécommunications (**IWGDPT**) a été organisée à Prague. Deux documents y ont été adoptés :

- Un document de travail sur le pistage en ligne et le respect de la vie privée : le respect du contexte, de la transparence et du contrôle reste essentiel.
- Un document de travail et des recommandations sur la publication de données à caractère personnel sur le Web, le référencement dans le contexte des sites Web et la protection de la vie privée.

La mise en œuvre du **projet de partenariat Leonardo da Vinci**, « Sensibilisation aux questions de protection des données parmi les employés travaillant au sein de l'UE », se poursuit. Le but est de préparer un manuel exhaustif destiné à un large public d'employés européens, et d'organiser des événements parallèles afin de sensibiliser le public. Les partenaires du projet sont les DPA polonaise (le coordinateur du projet), tchèque, bulgare et croate. Le projet devait être terminé en juillet 2014.

Organisation	Bureau de la protection des données à caractère personnel
Président et/ou collège	M. Igor Němec (président du bureau)
Budget	128 731 000 CZK (4 694 785 EUR, au taux de change de 1 EUR = 27,42 CZK)
Personnel	100
Activités générales	
Décisions, avis, recommandations	6 avis (la plupart concernant plus ou moins la surveillance des citoyens) 1 recommandation exhaustive – méthodologie pour des opérateurs

	de boutiques en ligne
Notifications	6 570 notifications (dont 5 994 enregistrées, et 576 toujours en cours ou suspendues)
Contrôles préalables	85
Demandes émanant de personnes concernées	2 994 (dont 15 de la part de personnes étrangères)
Plaintes émanant de personnes concernées	1 336 (plus 7 428 concernant des spams)
Conseils sollicités par le Parlement ou le gouvernement	Aucune activité de ce type en 2013
Autres renseignements relatifs aux activités générales	79 demandes relevant de la loi sur le libre accès aux informations. 69 projets de loi et 95 règlements d'application commentés dans le cadre de la procédure de commentaires interministérielle Autorisations de transferts internationaux : 25 demandes dont 20 autorisées, 1 refusée et 4 suspendues pour des raisons procédurales
Activités d'inspection	
Contrôles, enquêtes	90 (dont 74 ont abouti) + 91 enquêtes concernant des spams (toutes abouti)
Activités de sanction	
Sanctions	Env. 61 sanctions Note explicative : Par « sanctions », on entend toute mesure corrective non financière imposée à un responsable du traitement. Dans le cadre de nos enquêtes, nous avons souvent imposé un certain nombre de sanctions (mesures correctives) différentes. Toutefois, à toutes fins utiles et informatives, un ensemble de sanctions prises dans le cadre d'une enquête particulière ne sera décompté qu'une seule fois. La moyenne s'établit à environ 2,7 par action.
Amendes	Env. 155 amendes
DPD	
Chiffres relatifs aux DPD	Non applicable en République tchèque.

B. Informations sur la jurisprudence

Sur la base de plusieurs plaintes, nous avons mené une **enquête sur trois opérateurs de remonte-pentes** dans trois stations de ski différentes. Tous les skieurs étaient photographiés et mesurés par une puce laser à l'achat de leur ticket ou de leur forfait (les plaintes concernaient principalement les forfaits saisonniers). Les photographies ainsi que les noms et prénoms, la taille et le numéro du ticket, étaient stockés dans une base de données. L'objet déclaré était de prévenir l'utilisation abusive des forfaits (souvent utilisés par plusieurs personnes). Les skieurs étaient contrôlés lorsqu'ils se présentaient aux remonte-pentes (il était vérifié que les données correspondaient au ticket présenté). Les données étaient

effacées une fois la saison terminée. Les enquêtes ont révélé que tous les opérateurs (tous également responsables du traitement de données) violaient la loi en deux occasions : 1. En omettant d'informer les personnes concernées du traitement de leurs données, 2. En omettant de notifier le traitement et de s'inscrire auprès de la DPA tchèque. Nous avons par conséquent imposé des sanctions non financières aux trois opérateurs (qui ont été obligés de prendre les mesures correctives appropriées).

Nous avons enquêté auprès du côté tchèque d'**EURODAC**. L'inspecteur a choisi plusieurs dossiers au hasard et vérifié les procédures déployées sur place (il existe trois sites en République tchèque, où des empreintes digitales et autres données sont collectées et stockées). L'enquête n'a révélé aucune violation de la loi sur la protection des données. Le ministère de l'intérieur tchèque a néanmoins salué notre recommandation concernant la nécessité de mettre en place une meilleure communication rétroactive entre l'opérateur EURODAC et les bureaux de registres (des informations concernant un demandeur d'asile obtenant la citoyenneté grâce au mariage, par exemple).

En raison de nombreuses plaintes (concernant, notamment, la divulgation de données fausses ou incomplètes et la non-suppression de données illicites sur demande), nous avons réalisé **une enquête auprès du registre central des débiteurs (CERD)**. Nous avons découvert que l'entité n'était qu'un sous-traitant et que le responsable du traitement était établi aux États-Unis. L'enquête a révélé une violation de la loi sur la protection des données en deux occasions : 1. L'absence de collecte des données à caractère personnel uniquement aux fins déclarées et dans une mesure proportionnée à ces fins, 2. Le non-respect des droits de la personne concernée dans les cas concernant le traitement illicite de données. Nous avons imposé des mesures correctives au sous-traitant et l'avons obligé à nous informer de leur exécution. Nous avons également recommandé d'améliorer l'intelligibilité des services offerts afin de prévenir de nouvelles plaintes.

Nous avons mené une enquête sur la sécurité de données traitées dans le **système unifié d'informations sur le travail et les affaires sociales,** dont le responsable du traitement est le ministère du travail et des affaires sociales tchèque. Nous avons découvert que le système pouvait être utilisé par plusieurs fonctionnaires via un nom d'utilisateur et un mot de passe communs. Il pouvait également fonctionner sans qu'il soit nécessaire de se connecter. Nous avons par conséquent ordonné de prendre deux mesures correctives : 1. donner à chaque agent autorisé un nom d'utilisateur et un mot de passe propres, 2. s'assurer de l'introduction d'un protocole d'accès par le fournisseur du logiciel.

C. Autres informations importantes

Notre personnel d'encadrement a réalisé plusieurs enquêtes au sein de trois ambassades tchèques, parfois en marge d'un voyage d'affaires vers une conférence ou un autre événement.

En 2013, nous avons commencé une enquête en relation avec la migration de SIS 1+ vers SIS II, dans le but de vérifier la manière dont la police de la République tchèque, en tant que responsable du traitement des données dans ce système, assurait la protection des données à caractère personnel. L'enquête a porté sur les procédures ainsi que sur la sécurité technique et physique des données. L'enquête était toujours en cours en 2014.

Sensibilisation : nos experts ont donné 33 conférences sur la loi sur la protection des données au sein d'établissements publics, d'organes de l'administration locale et d'entités privées.

En 2013, nous avons préparé le lancement du nouveau site Web du bureau. Adapté sur le plan de la visibilité, ses fonctionnalités ont également été améliorées sans que sa structure ne soit modifiée afin de ne pas troubler les utilisateurs réguliers.

ROUMANIE

A. Résumé des activités et actualités

Organisation	Autorité nationale de contrôle du traitement des données à caractère personnel
Président et/ou collège	Ancuta Gianina Opre
Budget	3 460 000 RON (environ 772 321 EUR)
Personnel	43, plus la présidente et le vice-président de l'autorité
Activités générales	
Décisions, avis, recommandations	632 dont 5 décisions pour la suppression de données à caractère personnel, 1 décision de mettre un terme au traitement de données et de supprimer des données à caractère personnel traitées, et 1 recommandation
Notifications	7 499
Contrôles préalables	-
Demandes émanant de personnes concernées	156
Plaintes émanant de personnes concernées	721
Conseils sollicités par le Parlement ou le gouvernement	32
Autres renseignements relatifs aux activités générales	-
Activités d'inspection	
Contrôles, enquêtes	229 sur place et 44 par écrit
Activités de sanction	
Sanctions	66 amendes pour un montant total de 134 500 RON (environ 30 022 EUR)
Amendes	124 avertissements
DPD	
Chiffres relatifs aux DPD	-

B. Informations sur la jurisprudence

Jurisprudence 1

Un tribunal a divulgué les données à caractère personnel d'une victime d'une infraction pénale sans son consentement, dans un communiqué de presse émis par son porte-parole.

Le communiqué de presse a été diffusé en même temps par un réseau de télévision dans le cadre de son magazine d'information, avec un enregistrement vidéo de la déclaration publié sur le site web de cette même chaîne de télévision, accessible par tout visiteur.

Le représentant du responsable du traitement a déclaré que, dans son interview, le porte-parole avait cité un document rédigé conformément à l'énoncé des faits, où étaient mentionnés le nom et le prénom de la victime. Dans le communiqué de presse publié par la suite, les données d'identification de la victime ont été anonymisées par l'emploi des initiales de ses nom et prénom.

Le responsable du traitement a été sanctionné pour la contravention prévue par l'article 32 de la loi nº 677/2001.

Il a par ailleurs été recommandé au responsable du traitement de créer un document destiné à prouver la formation de ses porte-paroles en matière de protection des données des personnes concernées vis-à-vis des moyens de communication de masse.

Jurisprudence 2

Un requérant a déclaré avoir reçu de manière répétée des communications commerciales non sollicitées de la part d'une agence de voyages dont il dit n'avoir jamais utilisé les services. Le requérant a également mentionné le fait que ces messages commerciaux ne contenaient pas toutes les coordonnées de l'agence de voyages, qui a continué à lui envoyer des messages commerciaux même après qu'il avait utilisé le mécanisme de désinscription du contenu des messages afin de demander à ne plus les recevoir.

Suite à la vérification des messages commerciaux reçus par le requérant, il s'est avéré que ceux-ci n'indiquaient pas le nom exact d'une entreprise commerciale. L'autorité de protection des données a mené plusieurs enquêtes tant par écrit qu'auprès du siège de cette société. Elle a pu établir le refus des représentants de l'agence de voyages de lui fournir les informations demandées en exerçant ses pouvoirs d'enquête ainsi que la poursuite de la transmission de communications commerciales au requérant malgré son opposition répétée.

Compte tenu des conclusions, le responsable du traitement a été sanctionné sur la base de la loi nº 677/2001 et de la loi nº 506/2004 parce que la société a refusé de fournir les informations et de participer à l'enquête annoncée, a continué d'envoyer de manière répétée des communications commerciales au requérant bien qu'il n'ait jamais donné explicitement son consentement de recevoir ce type de communications commerciales. En outre, la plupart des messages ne contenaient pas toutes les coordonnées concernant l'identité réelle de l'envoyeur.

Jurisprudence 3

Le ministère de l'intérieur a informé l'autorité de protection des données de la divulgation de plusieurs catégories de données à caractère personnel sur Internet, et a envoyé, pour preuve, un dispositif optique sur lequel étaient stockés des documents contenant des données à caractère personnel.

De par cette notification, l'autorité de protection des données a été informée de l'existence de documents Internet (sur un réseau informatique à la demande) représentant différents actes notariés : adresses de différentes études de notaires, d'autorités publiques centrales/locales, contrats, mandats, déclarations de personnes physiques, déclarations de certains magistrats du parquet faisant référence à

leur non-coopération avec les services de renseignement ou leur non-appartenance à la police politique, documents d'authentification, etc.

Suite à l'enquête réalisée, le notaire à l'origine des documents a admis que ces documents étaient réels, avaient été rédigés sur les ordinateurs de ses employés, mais qu'il ne pouvait expliquer de quelle manière ils avaient été publiés sur Internet. D'après la déclaration du notaire, ces ordinateurs présentaient des problèmes de dysfonctionnement suite à l'attaque d'un virus.

À la date de l'enquête, il s'est avéré que cette étude notariale n'avait pas adopté de procédures internes assurant une sécurité minimale au traitement de données à caractère personnel malgré l'ordonnance nº 52/2002 prévoyant l'approbation des exigences de sécurité minimale en matière de traitement de données à caractère personnel.

D'après les conclusions, à la date de l'enquête, aucune méthode d'authentification n'était requise pour avoir accès aux ordinateurs sur lesquels les documents notariés étaient rédigés. D'un autre côté, les documents auraient pu être copiés sur tout support externe et imprimés par toute personne ayant accès à ces ordinateurs. L'inexistence de méthodes d'authentification indique que toute personne pouvait avoir accès à toutes les données à caractère personnel de tout ordinateur de cette étude notariale, et qu'il était dès lors impossible d'identifier dans les journaux les personnes qui avaient eu accès aux appareils informatiques. Par ailleurs, il était possible de copier tout document sur un dispositif externe et, par conséquent, d'infecter l'ordinateur par des virus transitant par les dispositifs de stockage externe utilisés.

Le responsable du traitement a été sanctionné pour la contravention prévue par l'article 33 de la loi nº 677/2001 parce qu'il n'avait pas adopté, à la date de l'enquête, de mesures de sécurité et de confidentialité suffisantes pour protéger les données à caractère personnel de ses clients, employés et collaborateurs (y compris les données sensibles) contre toute divulgation et tout accès non autorisé, ni contre aucune des formes de traitement illégal prévues aux articles 19 et 20 de la loi nº 677/2001, ce qui a permis la divulgation de ces données à caractère personnel sur Internet.

ROYAUME-UNI

A. Résumé des activités et actualités

L'ICO s'est fixé lui-même cinq objectifs clés. Nous avons sélectionné ci-dessous les principales activités que nous avons déployées pour les atteindre.

1. Les organisations comprennent mieux leurs droits et obligations en matière d'information.

L'ICO a publié des conseils sur

- les pratiques relatives à l'accès des personnes concernées ;
- le marketing direct ; et
- les analyses de l'impact sur la vie privée.

Nous avons également porté notre attention sur Care.data, un système destiné à permettre aux médecins généralistes britanniques de publier des informations médicales utilisées principalement à des fins de recherche médicale et faisant l'objet d'un examen minutieux. Notre intervention a permis d'améliorer l'information des patients et de réviser les échéances, mais, malgré les assurances, il est devenu clair que ces mécanismes n'étaient pas efficaces. Nous continuerons d'essayer de garantir la mise en place de mécanismes efficaces pour assurer le respect du choix des patients.

2. Les pouvoirs d'exécution sont utilisés de manière proportionnée pour améliorer la conformité aux droits à l'information.

Nous avons obtenu 12 condamnations pénales et émis deux avertissements dans le cadre de la poursuite du délit pénal d'obtention ou de divulgation illicite de données à caractère personnel.

3. Les clients reçoivent une réponse proportionnée, juste et efficace à leurs préoccupations en matière de droits à l'information.

Cette année, nous avons reçu et clos un nombre record de dossiers. L'ICO reste déterminé à améliorer les pratiques en matière de droits à l'information en s'appuyant sur les préoccupations des personnes pour élargir ces améliorations. Nous avons par exemple demandé un plan d'action à l'autorité bancaire britannique, après que la demande d'une personne pour obtenir ses propres informations a pris plus de neuf mois avant d'être résolue. Nous nous sommes par ailleurs assurés qu'AXA PPP Healthcare réviserait ses procédures d'obtention d'un consentement approprié dans le cadre du traitement d'informations médicales.

4. Les personnes sont en mesure d'exercer leurs droits à l'information.

L'accès des personnes concernées est l'une des pierres angulaires de la loi sur la protection des données. Toutefois, ce droit a, depuis un certain temps, fait l'objet d'une utilisation abusive de la part d'organisations obligeant des personnes à demander des informations personnelles avant de les révéler à l'organisation. Cet accès obligatoire des personnes concernées est une perversion des droits des personnes et, bien que des dispositions aient été inclues à la loi de 1998 sur la protection des données afin de faire appliquer des sanctions pénales, celles-ci ne l'ont jamais été.

Nous avons continué de faire pression en faveur d'un changement, et le nouveau ministre de la justice, le député Simon Hughes, a depuis confirmé que d'autres récents changements de la loi avaient supprimé les obstacles et qu'il est possible d'ériger en infraction l'obligation d'accès des personnes

concernées. Nous travaillons avec le ministère de la justice et les autres ministères concernés afin de veiller à ce que cette possibilité soit mise en œuvre.

5. L'ICO est vigilant et réceptif aux changements qui impactent les droits à l'information.

Nous avons formulé des conseils sur la révision proposée du régime européen de protection des données aux fonctionnaires du ministère de la justice et aux membres du Parlement européen, et avons coopéré avec le groupe de travail « Article 29 ». Nous avons publié une analyse approfondie des dernières propositions sur notre site web.

Nous avons également publié nos recherches sur l'impact de la révision proposée sur les entreprises, qui ont mis en lumière l'incertitude de nombreuses estimations de coûts utilisées lors des débats :

- 40 % d'entreprises n'ont bien compris aucune des dix dispositions proposées et
- 87 % étaient incapables d'estimer le coût des propositions pour leur activité.

Au cours de l'année, nous avons demandé des conseils sur la faisabilité de l'accréditation par l'ICO d'une tierce partie pour que celle-ci mette en place un système de certification ou de sceaux de confidentialité. Nous avons notamment coopéré en ce sens avec le service d'accréditation britannique. Une annonce sur le système proposé par l'ICO sera faite en 2014-2015.

6. Un ICO efficace et bien préparé pour l'avenir.

De nouvelles initiatives importantes introduites cette année nous ont aidés à travailler de manière plus efficace et à proposer au public des services améliorés :

Nos nouveaux système et service d'inscription ont facilité la compréhension du registre public des responsables du traitement des données par ses visiteurs. Ils sont également plus faciles à utiliser pour ceux qui ont besoin de s'inscrire, et nous avons fini l'année en lançant un service d'inscription complet en ligne.

Nous avons apporté des améliorations à notre système téléphonique afin de répondre à l'augmentation des demandes. Nous pouvons désormais orienter les appelants vers le membre du personnel adéquat de manière plus efficace et, si vous nous appelez en dehors des heures de travail, nous disposons aussi d'un service automatique amélioré.

Au cours de l'année, nous avons été de plus en plus proactifs dans la divulgation d'informations sur notre travail opérationnel.

Organisation	Bureau du commissaire à l'information
Président et/ou collège	M. Christopher Graham (commissaire)
Budget	Environ 21 millions (frais de notification de 16,5 M GBP et 4,25 M GBP de subvention pour la liberté d'information)
Personnel	370 ETP
Activités générales	
Décisions, avis, recommandations,	pratiques sur l'accès des personnes concernées marketing direct

	évaluations de l'impact sur la vie privée
Notifications	Nombre total de responsables de données notifiés : 389 036
Contrôles préalables	S. o.
Demandes émanant de personnes concernées	Appels sur la ligne d'assistance téléphonique : 259 903
Plaintes émanant de personnes concernées	Nombre de plaintes reçues dans le domaine de la protection des données : 13 760 Nombre de plaintes reçues dans le domaine de la liberté d'information : 4 688 Nombre de plaintes reçues dans le domaine de la loi sur la protection de la vie privée et les communications électroniques : 161 720
Conseils sollicités par le Parlement ou le gouvernement	Réponses données à 44 consultations
Autres renseignements relatifs aux activités générales	Aucun
Activités d'inspection	
Contrôles, enquêtes	63 audits (et 117 visites consultatives)
Activités de sanction	
Sanctions	Enquêtes dans 1 755 cas de protection des données 7 avis d'exécution et 20 engagements. Poursuites : 15 (1 cas ayant entraîné la confiscation de fonds pour un total de 73 000 GBP à rembourser)
Amendes	Amendes civiles émises à hauteur de 1,97 M de GBP
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

S. o.

C. Autres informations

Les autres principaux éléments importants sont les suivants :

Prêts aux étudiants

La vente du portefeuille de prêts aux étudiants au secteur privé aurait pu donner lieu à la divulgation aux agences d'évaluation de crédit d'un grand nombre d'informations non nécessaires sur les prêts. Nous

nous sommes efforcés à ce que les informations concernant des comptes à jour ne soient pas transférés à ces agences, et qu'il existe des garanties efficaces pour assurer l'exactitude de toutes les informations transférées.

Services de rencontres en ligne

L'utilisation de services de rencontres en ligne s'est développée, et des inquiétudes ont été soulevées quant aux informations personnelles utilisées et partagées. Nous avons initié un travail avec l'association des rencontres en ligne afin de développer des conseils pour le secteur.

Télévisions connectées à Internet

Nous sommes en contact avec un fabricant de postes de télévision afin de répondre à des inquiétudes selon lesquelles les informations sur les habitudes des téléspectateurs seraient collectées par l'intermédiaire de postes de télévision connectés à Internet, même en cas d'activation des paramètres de respect de la vie privée.

Associations caritatives et groupes communautaires

Nous avons travaillé avec des associations caritatives et des groupes communautaires qui apportent leur soutien à certaines des personnes les plus vulnérables de la société en organisant des présentations, des visites consultatives et des ateliers.

The Consulting Association

Une initiative importante pour nous cette année avait trait à une affaire que nous avions eu à gérer en 2009. Suite à la saisie de dossiers de The Consulting Association, l'ICO était en possession d'informations qui avaient servi de liste noire dans le secteur de la construction.

Outre la résolution des problèmes de protection des données que cette situation impliquait, nous avions à cœur de contacter les personnes qui avaient ainsi pu être inscrites sur cette liste noire. Dans de nombreux cas, compte tenu du temps écoulé, il nous semblait peu probable que les informations que nous détenions nous permettraient d'identifier précisément des personnes. Toutefois, en coopérant avec Equifax et le département du travail et des retraites, nous avons pu identifier les coordonnées d'un certain nombre de personnes inscrites dans ces dossiers.

De nombreux autres employés, anciens et actuels, du secteur de la construction et leurs représentants nous ont contactés afin de savoir si leurs coordonnées figuraient dans les dossiers saisis. Entre 2009 et le 31 mars 2014, nous avons fourni des informations pertinentes à 776 personnes. Sur ce nombre, 461 personnes ont été informées sur l'année de référence 2013/14.

Travailler pour améliorer la cohérence et la coordination dans les enquêtes et l'application de la protection des données à l'international

L'ICO joue également un rôle primordial dans l'amélioration de la coordination de la mise en application avec d'autres autorités de régulation du respect de la vie privée :

Nous avons coprésidé un groupe de travail sur la coordination internationale de la mise en application qui a donné lieu à l'adoption d'une résolution visant à faire progresser ce travail, à l'occasion de la conférence internationale des commissaires à la protection des données et de la vie privée. Nous assurons aujourd'hui le développement d'un ensemble de règles d'échange d'informations concernant les activités de mise en application.

Nous siégeons au comité exécutif du Global Privacy Enforcement Network (GPEN).

Nous sommes représentés dans le groupe de travail de l'OCDE sur la sécurité et la vie privée dans l'économie numérique, où nous contribuons à son travail de mise à jour des lignes directrices de l'OCDE sur la protection de la vie privée, désormais adoptées par le Conseil de l'OCDE.

Nous avons signé un protocole d'accord avec la Federal Trade Commission américaine et un autre avec l'autorité du centre financier international de Dubaï.

Changements dans la manière dont nous traitons les plaintes

Au cours de l'année, nous avons entrepris d'importants travaux de préparation, y compris de consultation, avant d'apporter d'importants changements, en avril 2014, à la manière dont nous traitons les plaintes et dont nous gérons les inquiétudes du public. Ces changements nous permettront d'adopter une approche plus collaborative et proportionnée de ce domaine important de notre travail réglementaire.

SLOVAQUIE

A. Résumé des activités et actualités

Le premier semestre de 2013 a été caractérisé par la poursuite des efforts déployés pour modifier la législation sur la protection des données et le second semestre par la mise en pratique des lois adoptées. S'appuyant sur le plan des tâches législatives du gouvernement de la République slovaque pour le second semestre 2012, le bureau de protection des données à caractère personnel de la République slovaque (ci-après, le « bureau ») a préparé un tout nouveau projet de loi sur la protection des données à caractère personnel. Cette modification législative avait pour objectif la transposition complète de la directive 95/46/CE du Parlement européen et du Conseil, et la mise en œuvre des conclusions et des recommandations de l'évaluation de Schengen en République slovaque en matière de protection des données à caractère personnel et d'analyse des lois du point de vue de leur application pratique. Ce processus législatif s'est terminé en avril 2013 lorsque le Parlement national slovaque a adopté une nouvelle loi sur la protection des données à caractère personnel sous le numéro 122/2013 Coll.

La loi entrée en vigueur le 1er juillet 2013 est synonyme d'importants changements, tels qu'une meilleure spécification du statut des responsables du traitement et des sous-traitants, ainsi que des relations qui les lient. Elle réglemente désormais les exigences applicables au traitement de données biométriques, définit clairement le champ d'application et la documentation des mesures de sécurité, et spécifie l'établissement de la personne habilitée (qui entre en contact avec les données à caractère personnel chez le responsable du traitement). Par ailleurs, elle réglemente désormais les exigences applicables à la désignation d'un délégué à la protection des données (la nouvelle loi sur la PDP rend obligatoire la réussite à un examen pour exercer cette fonction au bureau), renforce les mécanismes de protection des droits des personnes concernées, modifie les conditions des flux transfrontaliers de données à caractère personnel, spécifie les conditions de notification et d'enregistrement spécial des systèmes d'archivage, introduit des frais administratifs d'enregistrement spécial, précise la position du bureau, et en étend les compétences dans le domaine de la protection des données à caractère personnel, etc.

Le bureau a poursuivi la prestation de services hebdomadaires de contrôle et d'évaluation des documents inclus au processus législatif dans le cadre des procédures d'examen interministérielles. Ce processus a pour objet de suivre tous les documents inclus aux procédures d'examen interministérielles et, par conséquent, d'évaluer et de commenter ces documents de manière efficace. Pour tout document proposé, le bureau a évalué la conformité avec la loi sur la protection des données à caractère personnel, afin d'assurer la protection juridique des exigences de base de la vie sociale tout en minimisant les interférences avec le droit à la vie privée et le respect de la vie privée des personnes. À ces fins, chaque projet de législation qui, par son contenu, régit le traitement de données à caractère personnel, doit respecter les exigences de base de la loi sur la protection des données à caractère personnel.

L'adoption et la mise en œuvre d'une nouvelle loi sur la protection des données à caractère personnel a accru l'intérêt de tous les acteurs de la protection des données à caractère personnel. Les demandes d'informations sur ce sujet ont énormément augmenté au second semestre de 2013. Le bureau a dû répondre par écrit à 2 263 demandes au total, dont 1 671 portant sur la nouvelle loi. Les réponses téléphoniques se comptent quotidiennement par dizaines. L'obligation de réussir un examen du bureau pour les personnes souhaitant exercer une fonction de DPD a également contribué à accroître l'intérêt et les discussions, et à améliorer la protection des données. Le bureau a organisé une formation à l'attention des responsables du traitement, des sous-traitants, des DPD ou des personnes habilitées à travers tout le pays afin de satisfaire aux exigences de connaissance de la loi.

Activités d'inspection du bureau à l'échelle nationale

En 2013, le bureau a réalisé plusieurs opérations d'inspection à l'échelle nationale sur la base du plan annuel des activités de contrôle et à l'initiative de personnes concernées, d'autorités publiques ou d'autres personnes. Le plan d'activités de contrôle annuelles s'est focalisé sur les inspections relatives au traitement de données à caractère personnel dans des systèmes d'archivage et, par exemple, dans le domaine des services sociaux, des autorités autonomes locales, des services financiers ou de la vidéosurveillance. Étant donné que les lois nationales ont changé vers le milieu de 2013, les inspections ont été divisées en deux parties. La première partie a été réalisée en vertu de la loi nº 428/2002 Coll. et la seconde en vertu de la loi nº 122/2013 Coll. sur la protection des données à caractère personnel en raison de la différence des dispositions sur les inspections et les procédures de contrôle.

L'unité nationale du SIRENE

En vertu de la 3e disposition du plan d'action de Schengen de la République slovaque, le bureau a enquêté sur la licéité du traitement de données à caractère personnel dans le Système d'information Schengen de deuxième génération, que la République slovaque a rejoint le 9 avril 2014. L'inspection avait pour but de contrôler la conformité du traitement de données dans un cadre juridique approprié, ainsi que la sécurité des données à caractère personnel traitées. Le bureau a également contrôlé l'étendue des données à caractère personnel traitées concernant des personnes recherchées par la police à des fins de remise ou d'extradition, concernant des résidents de pays tiers dans le cadre d'un refus d'entrée ou de séjour, et concernant des personnes et marchandises aux fins d'une surveillance discrète ou de contrôles spécifiques. Le bureau a révélé que la sécurité du traitement de données à caractère personnel relevait d'un haut niveau et respectait totalement le cadre juridique adéquat.

Le domaine des services sociaux

Le bureau a axé ses activités de contrôle en 2013 sur des domaines où les responsables du traitement traitent non seulement des données à caractère personnel générales, mais également des données relevant de catégories particulières. Le domaine des services sociaux exige du bureau une attention particulière en raison de toutes les organisations (responsables du traitement) concernées qui traitent d'importantes quantités de données relevant de catégories particulières. Les contrôles dans ce domaine ont fait suite aux contrôles de l'année précédente et ont montré que les responsables du traitement avaient négligé de respecter certaines obligations administratives relevant de la loi nº 428/2002 Coll., telles que les obligations d'informer de leurs obligations les personnes responsables travaillant avec des données à caractère personnel, de conserver un registre lors de l'utilisation de fichiers, ou de ne pas désigner un délégué à la protection des données, etc. Le bureau a émis plusieurs mesures correctives et lancé une procédure visant à imposer une amende après cinq contrôles.

Autorités autonomes locales

Conformément à de nombreuses lois nationales, les autorités autonomes locales appartiennent à un type de responsables du traitement qui traitent des catégories particulières de données. Elles tiennent à jour un registre des citoyens, collectent les droits et honoraires locaux, assurent le versement des prestations d'aide sociale et fournissent d'autres services municipaux, etc. L'ensemble de ces activités requièrent le traitement de catégories particulières de données, et les autorités autonomes locales peuvent reconnaître les situations économique, sociale, raciale ou sanitaire des personnes concernées. Le bureau a effectué 10 contrôles, dont 9 ont donné lieu à un protocole de mesures correctives. Outre le non-respect de leurs obligations administratives, les responsables du traitement avaient publié les numéros d'identification personnels de personnes concernées sur leurs sites web, divulgué la situation économique de personnes concernées lors de sessions du parlement local, omis d'indiquer qu'un espace public était surveillé par des caméras de vidéosurveillance et, dans un cas, le responsable du traitement n'avait respecté aucune de ses obligations juridiques.

Services financiers

Le bureau a effectué 3 contrôles en vertu de la loi nº 428/2002 Coll. et 8 contrôles en vertu de la loi nº 122/2013 Coll. dans le domaine des services financiers. Les responsables du traitement avaient traité des données à caractère personnel en se référant principalement à la loi spéciale nº 186/2009 Coll. sur le courtage et le conseil financiers. Cette loi autorise le traitement de données dans des catégories particulières, et c'est la raison pour laquelle le bureau a accru la surveillance de ce secteur. Les principaux problèmes avaient trait au traitement de données par un sous-traitant, à la détermination du champ d'application et des conditions du traitement, à la collecte et au traitement en conflit avec la loi, et à l'utilisation des données à des fins différentes sans en notifier la personne concernée.

Flux transfrontalier de données à caractère personnel

La loi nº 122/2013 Coll. a également changé les conditions des flux transfrontaliers de données. Le concept a été retravaillé afin d'adhérer plus étroitement à la nouvelle version, qui autorise un plus haut niveau de flexibilité et réduit la charge administrative. La loi distingue bien évidemment les transferts vers les États membres de l'Union européenne et les pays qui sont parties à l'accord sur l'Espace économique européen, et autorise des transferts vers des pays tiers dans le cas où il existe une décision de la Commission européenne selon laquelle le pays en question assure un niveau adéquat de protection des données à caractère personnel. Elle prévoit également des transferts de données vers des pays tiers qui n'assurent pas un niveau de protection des données adéquat. Les cas de flux transfrontaliers de données au sein de l'UE et vers de pays tiers doivent également assurer un niveau de protection adéquat. La loi requiert uniquement l'existence d'une base juridique applicable pour la réalisation de cette opération de traitement, et le responsable du traitement doit informer la personne concernée de ce transfert, et s'assurer la sécurité de ses données lors du transfert. Ce type de transfert transfrontalier ne connait aucune autre limitation. Des données peuvent être transférées vers un pays tiers qui n'assure pas un niveau de protection adéquat uniquement si le responsable du traitement prévoit suffisamment de garanties pour la protection de la vie privée, des droits fondamentaux et des libertés des personnes. Les règles d'entreprise contraignantes et les clauses contractuelles standard sont considérées comme étant des garanties suffisantes pour ces transferts.

Le niveau de la charge administrative a été réduit par un nouveau mécanisme d'autorisation préalable des transferts transfrontaliers vers un pays tiers qui n'assure pas un niveau de protection adéquat. Par le passé, le responsable du traitement devait demander une autorisation préalable pour tous les transferts vers un pays tiers ne relevant pas d'une décision adéquate en vertu de la loi nº 428/2002 Coll. Il est désormais nécessaire de demander une autorisation du bureau uniquement dans les cas où le responsable du traitement intervient dans le contenu de clauses contractuelles standard ou les cas d'apparente contradiction.

Organisation	Bureau de protection des données à caractère personnel de la République slovaque
Président et/ou collège	Mme Eleonóra Kročianová, présidente
Budget	876 324 €
Personnel	33 employés
Activités générales	
Décisions, avis, recommandations	Le bureau a émis les six recommandations suivantes en 2013 : 1/2013 Le concept de données à caractère personnel 2/2013 Concepts de base – personnes impliquées dans le traitement de données à caractère personnel

	3/2013 Caméras de vidéosurveillance dans les véhicules privés 4/2013 Transfert transfrontalier de données à caractère personnel 5/2013 Le concept des fichiers 6/2013 Traitement de données biométriques
Notifications	387
Contrôles préalables	28
Demandes émanant de personnes concernées	160 plaintes et demandes émanant de personnes concernées 34 plaintes et demandes émanant d'autres personnes
Plaintes émanant de personnes concernées	
Conseils sollicités par le Parlement ou le gouvernement	108
Autres renseignements relatifs aux activités générales	Le bureau a délivré 7 discours à la radio, 9 à la télévision nationale et 58 contributions à la presse.
Activités d'inspection	
Contrôles, enquêtes	163 contrôles
Activités de sanction	
Sanctions	151 décisions de mesures correctives
Amendes	11 amendes pour un total de 25 160 € 9 amendes pour des délits administratifs pour un total de 20 360 € 2 amendes pour un total de 3 500 €
DPD	
Chiffres relatifs aux DPD	Le bureau a réalisé 253 examens de DPD pendant son établissement et 47 dans d'autres parties du pays pour 3 073 demandeurs au total, et émis 1 705 certificats de réussite aux tests.

B. Informations sur la jurisprudence

Le système juridique de la République slovaque, comme les systèmes juridiques de plusieurs autres États membres, ne s'appuie pas sur la jurisprudence.

C. Autres informations importantes

Coopération internationale

Au niveau international, les travaux découlaient principalement de l'adhésion à l'Union européenne et aux groupes de travail établis sous l'égide et à partir d'actes juridiques des Communautés européennes,

ainsi que de demandes de partenariat et de coopération de la DPA. Le bureau a participé à toutes les réunions organisées par le Conseil de l'Europe, le Conseil de l'Union européenne ou la Commission européenne en 2013. Outre les réunions régulières des groupes de travail, le bureau a assisté à la conférence des autorités de protection des données d'Europe centrale et de l'Est, à la conférence de printemps à Lisbonne et à l'atelier de traitement des dossiers à Sarajevo. Elle a également organisé une réunion bilatérale avec la DPA de la République tchèque. Les deux DPA ont essayé de trouver des cas présentant des problèmes communs pouvant faire l'objet d'enquêtes coordonnées, et ont signé un protocole d'accord à la fin de la réunion.

SLOVÉNIE

A. Résumé des activités et actualités

L'année 2013 a été celle du dixième anniversaire des opérations pour le commissaire à l'information, dont le rôle s'est développé au fil des années, passant d'un petit organe d'appel dirigé par le commissaire à l'accès aux informations publiques, à un garant important de la transparence et un protecteur des données à caractère personnel. 2013 a également vu l'accomplissement de nombre de jalons importants qui nous ont aidés à comprendre tout ce que l'on peut perdre lorsque l'on abandonne sa vie privée. Des incidents notables, liés à des intrusions dans la vie privée, ont révélé que des intrusions majeures dans notre vie privée ont lieu chaque jour et que nous sommes impuissants, en tant que personnes, si l'État perd le contrôle dans ce domaine.

En 2013, le commissaire à l'information a reçu 106 demandes d'avis sur des propositions législatives et autres règlements qui prévoient la collecte et le traitement de données à caractère personnel (soit 26 de plus qu'en 2012). Nous avons détecté un nombre inquiétant d'amendements de lois et de propositions de nouvelles lois qui permettraient de graves intrusions dans la vie privée des personnes en termes de traitement de données à caractère personnel, qui sont adoptés par le biais de procédures rapides sans les analyses et évaluations appropriées de leurs conséquences destinées à s'assurer de leur constitutionnalité et de la garantie de la protection de la vie privée et des données à caractère personnel. Parmi les lois modifiées, citons la loi de procédure pénale, la loi sur le prélèvement et la transplantation d'organes humains à des fins de traitement médical, la loi sur le marché du commerce électronique, la loi sur la prévention de l'emploi et du travail non déclaré, la loi sur la santé et l'assurance santé, la loi sur les droits des patients, la loi sur les délits mineurs et la loi générale sur la conservation des données sur la base du paragraphe 4 de l'article 165 de la loi sur les communications électroniques.

Sur l'année écoulée, dans chacun de ses domaines d'activité, le commissaire à l'information a une fois encore reçu un grand nombre (record) de demandes de personnes, dont des demandes d'avis, des plaintes et des appels. D'un côté, cette augmentation est gratifiante, dans la mesure où elle indique clairement que les personnes ont de plus en plus conscience de l'objet et de l'importance des droits humains traités dans le cadre des compétences du commissaire. Dans le même temps, nous ne pouvons ignorer le fait que, une fois encore cette année, l'augmentation marquée du nombre de plaintes et de contrôles réalisés peut être attribuée à une tendance au maintien de pratiques troublantes de la part des autorités responsables dans le domaine de l'accès aux informations publiques, tandis que, d'un autre côté, nous sommes confrontés aux appétits de plus en plus difficilement gérables de nombreux responsables du traitement des données, tant privés que publics, impatients de collecter et de traiter des données à caractère personnel.

La réponse des personnes concernées confirme l'efficacité du travail du commissaire. Le centre d'étude de l'opinion publique Politbarometer a réalisé un sondage d'opinion publique en janvier 2013, qui comprenait une évaluation des performances des autorités de contrôle nationales. Ce sondage d'opinion publique a révélé que les performances de plusieurs autorités de contrôle indépendantes (y compris le commissaire à l'information) sont jugées de manière extrêmement positive par les personnes interrogées (par opposition à l'évaluation du fonctionnement des organes de l'État central – Assemblée nationale, gouvernement et président du gouvernement). Il convient par ailleurs de ne pas ignorer que le commissaire à l'information a également été classé parmi les institutions du gouvernement central et sociales auxquelles les Slovènes font le plus confiance dans les sondages d'opinion publique en 2010, 2011 et 2012, ce qui démontre une confiance établie du public dans le travail du commissaire à l'information.

Concernant le domaine de la protection des données à caractère personnel pour l'année 2013, le commissaire à l'information a traité 712 dossiers de contrôle et 106 procédures de délits. En 2013, le commissaire a vu s'accroître ses compétences de contrôle et d'inspection sur la législation qui réglemente les cookies. Mi-juin 2013, les dispositions sur les cookies de la loi sur les communications

électroniques, qui ont trait à la conservation des informations ou à la possibilité d'accéder à des informations stockées sur le terminal d'un abonné ou d'un utilisateur, sont entrées en vigueur. Après l'entrée en vigueur des dispositions sur les cookies, le commissaire à l'information avait, fin 2013, reçu 35 plaintes relatives à 141 organisations responsables (opérateurs de sites web). Les plaintes avaient principalement trait à l'inadéquation, voire l'absence totale, de mécanismes de notification et d'obtention du consentement. Les sites web n'offraient pas toujours des mécanismes de contrôle adéquats qui autoriseraient ou interdiraient véritablement l'installation de cookies. En particulier, plusieurs cas ont été observés où un site web avait installé des cookies pour lesquels, suite à l'entrée en vigueur des nouvelles dispositions de la loi sur les communications électroniques, le consentement explicite de l'utilisateur était requis. Les plus problématiques n'étaient pas seulement les cookies publicitaires et analytiques, mais également les cookies de certains modules d'extension généralement installés par des tierces parties et qui permettaient le pistage des activités de navigation quotidiennes des utilisateurs sur différents sites web (ou « cookies de pistage »). La grande majorité des organisations responsables contre lesquelles le commissaire à l'information a ouvert des procédures de contrôle, ont corrigé les irrégularités ou violations identifiées immédiatement après en avoir été informées, et le commissaire à l'information n'a dès lors pas eu à émettre de décisions réglementaires. En coopération avec les entités responsables, le commissaire à l'information a développé des lignes directrices sur l'utilisation de cookies, ainsi que des réponses aux questions les plus fréquentes, qui ont été publiées sur les pages web du commissaire à l'information. Nous avons reçu de nombreuses questions de la part d'opérateurs de sites web sur l'analytique web et, notamment, sur sa mise en œuvre de manière à être autorisée sur la base d'un consentement implicite à l'occasion de la première visite. Le commissaire à l'information a réussi à supprimer certains des modules d'extension les plus intrusifs, principalement imputables à des sites web du secteur public et de grands médias slovènes.

Outre les plaintes en lien avec les cookies déposées sur la période considérée, en 2013, comme les années précédentes, le plus grand nombre de plaintes reçues par le commissaire à l'information avaient trait à la vidéosurveillance et à l'utilisation de données à caractère personnel à des fins de marketing direct. Outre les plaintes susmentionnées, une attention particulière doit être portée aux plaintes déposées pour le transfert et, par conséquent, la lecture de courriels envoyés sur les adresses professionnelles des employés d'une société, aux plaintes déposées en raison de la publication de données à caractère personnel sur les sites web de responsables du traitement des données, aux plaintes déposées pour l'envoi de SMS payants et aux plaintes déposées pour le traitement de données inexactes et périmées.

De nouveaux défis de protection des données à caractère personnel continuent de se présenter dans le domaine des technologies modernes de l'information et de la communication. Ces défis concernent essentiellement l'utilisation plus répandue de systèmes automatiques pilotés à distance, qui permettent une collecte dissimulée, difficile à détecter et extensive de données à caractère personnel et d'importantes intrusions dans la vie privée. Ces systèmes automatiques pilotés à distance pouvant être équipés de nombreux outils de capture de vidéos, d'images, de sons et de données sur la température, le mouvement, la localisation, etc., et leur utilisation représentera un défi majeur pour les régulateurs comme pour les garants de la vie privée.

Une part importante des activités du commissaire à l'information relève également de l'introduction de nouveaux pouvoirs octroyés aux services répressifs, notamment au regard des changements très fréquents de la réglementation en matière de procédures pénales.

Le commissaire à l'information note que l'interprétation de la notion de confidentialité des communications reste difficile, et souligne qu'une demande écrite d'une autorité publique ne suffit pas pour obtenir des informations sur l'identification des personnes en communication, ce domaine relevant des dispositions de l'article 37 de la Constitution de la République de Slovénie. L'article prévoit que la confidentialité de la correspondance et d'autres moyens de communication soit garantie, et que la protection de la confidentialité de la correspondance et d'autres moyens de communication, ainsi que l'inviolabilité de la vie privée ne puissent être suspendues que sur la base d'une ordonnance d'un tribunal lorsque nécessaire pour l'ouverture ou au cours de procédures pénales, ou pour des raisons de sécurité nationale. Fin 2013, le commissaire à l'information a publié un rapport révélant des pratiques

dérangeantes de la police qui, en 2012, malgré les dispositions précises de la loi sur le marché du commerce électronique et de la loi de procédure pénale, avait demandé, sur la base de 35 demandes écrites, les données de prestataires de services de la société de l'information concernant des utilisateurs de sites web dont les contenus sont fournis ou transmis par des utilisateurs du service. Dans 31 cas, ces demandes avaient été faites sans l'ordonnance du tribunal pourtant nécessaire, tandis que 30 % des demandes écrites ne relevaient pas de l'infraction pénale en question.

Organisation	Commissaire à l'information de la République de Slovénie
Président et/ou collège	Mme Nataša Pirc Musar
Budget	1 291 010 EUR
Personnel	32 employés : direction (2 à 6 des employés sont également des contrôleurs, et 2 des conseillers juridiques), administratifs (3), conseillers juridiques sur l'accès aux informations publiques et la protection des données (10), chercheurs (2), contrôleurs de la protection des données (10) et 1 administrateur système.
Activités générales	Protection des données et accès aux informations publiques
Décisions, avis, recommandations	71 avis et recommandations exhaustifs et 2 389 avis et recommandations concis sur la base de demandes émanant de personnes concernées ou de responsables du traitement des données.
Notifications	134 notifications relatives à des fichiers de données à caractère personnel.
Contrôles préalables	23 contrôles préalables : 11 sur des données biométriques, 16 sur le transfert de données vers des pays tiers et 5 sur le regroupement de fichiers.
Demandes émanant de personnes concernées	2 460 demandes d'avis ou d'éclaircissements de la part de personnes concernées.
Plaintes émanant de personnes concernées	Au total, 852 plaintes émanant de personnes concernées. Domaines : 68 plaintes concernant le transfert ou la divulgation illicite de données, 43 concernant la collecte illicite de données, 28 concernant des cookies, 26 concernant la sécurité inadéquate des données, 15 concernant une vidéosurveillance illicite et une utilisation inappropriée d'images vidéo et 7 concernant le marketing direct. En outre, 63 plaintes concernant les droits de personnes concernées ont également été traitées.
Conseils sollicités par le Parlement ou le gouvernement	Le législateur et les autorités compétentes chargées de rédiger la législation ont consulté le commissaire au sujet de 106 lois et autres textes juridiques, tels que la loi de procédure pénale, la loi sur le prélèvement et la transplantation d'organes humains à des fins de traitement médical, la loi sur le marché du commerce électronique, la loi sur la prévention de l'emploi et du travail non déclaré, la loi sur la santé et l'assurance santé, la loi sur les droits

	des patients, la loi sur les délits mineurs et la loi générale sur la conservation des données sur la base du paragraphe 4 de l'article 165 de la loi sur les communications électroniques.
Autres renseignements relatifs aux activités générales	En 2013, le commissaire : - a poursuivi, en collaboration avec le centre slovène pour un Internet plus sûr, son travail de prévention (exposés, conférences) concernant l'utilisation sûre d'Internet pour les enfants, les élèves, leurs parents et enseignants ; - a poursuivi l'éducation des entités responsables et participé à divers ateliers, conférences, et tables rondes éducatives ; - a publié des lignes directrices sur l'analyse intelligente de la vidéo et des lignes directrices sur l'utilisation de cookies sur les sites web ; - a été consulté sur un certain nombre de lois ; - a poursuivi son engagement et sa participation active à de nombreux projets internationaux.
Activités d'inspection	
Contrôles, enquêtes	712 contrôles : 253 dans le secteur public, 459 dans le secteur privé.
Activités de sanction	
Sanctions	106 procédures de délits ouvertes (18 dans le secteur public, 62 dans le secteur privé, 26 personnes physiques), ayant notamment donné lieu à 26 avertissements et 72 décisions relatives à des violations (36 réprimandes et 36 amendes).
Amendes	La DPA a imposé des amendes à hauteur de 224 592 329 EUR, hors taxes administratives.
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

Enregistrements de conversations téléphoniques par un établissement public

Le commissaire à l'information a ouvert une procédure de contrôle à l'encontre d'un établissement public après avoir établi que, en tant qu'autorité responsable, il avait installé un système d'information automatique pour les appels sur le numéro de son centre de contact qui, avant de permettre aux appelants de parler à un responsable du centre de contact, les informaient que leur conversation serait enregistrée afin d'assurer la qualité des services. La procédure de contrôle a établi que l'autorité responsable avait introduit l'enregistrement des appels téléphoniques dans le but de maintenir et d'améliorer la qualité de ses services. Les enregistrements audio de conversations téléphoniques servaient à préparer des propositions pour un programme de formation d'opérateurs de centre d'appels (formation rhétorique, gestion des clients dans des situations difficiles, etc.). Le commissaire a conclu

que, malgré l'avertissement préalable de l'enregistrement, l'autorité responsable ne s'appuyait sur aucune base juridique pour ces enregistrements particuliers. Par conséquent, le commissaire à l'information a ordonné à l'autorité de mettre un terme à l'enregistrement des conversations téléphoniques sur le numéro de son centre d'appels, de détruire les enregistrements stockés et d'arrêter d'utiliser la notification automatique du système d'information stipulant que « votre appel sera enregistré pour assurer la qualité de nos services ».

Sécurité inadéquate des données à caractère personnel sensibles par un établissement de santé

Le commissaire à l'information a fait une visite de contrôle dans un établissement de santé, dont le but était de vérifier l'adéquation des procédures et des mesures de protection des données à caractère personnel. Lors de ce contrôle, le commissaire à l'information s'est aperçu que les documents internes régulant la sécurité des données à caractère personnel ne déterminaient pas de procédure visant à conserver ou à utiliser des pistes d'audit des accès aux données à caractère personnel. Le commissaire à l'information a conclu que, dans sa base de données à caractère personnel, l'autorité responsable traitait de grandes quantités de données à caractère personnel, dont une grande part était, au regard du domaine d'activité de l'autorité, des données à caractère personnel sensibles, dont l'utilisation abusive pourrait avoir des conséquences graves, chronophages et, dans certains cas, irréversibles pour la personne. Compte tenu de la sensibilité des données traitées par l'autorité responsable, toute analyse des risques aurait dû démontrer que ces données présentaient un niveau élevé, et probablement le niveau de risque le plus élevé et que, par conséquent, des mesures et procédures de protection de ces données à caractère personnel auraient dû être mises en place au plus haut niveau afin de réduire les risques auxquels elles sont exposées. Le commissaire à l'information a par conséquent ordonné à l'autorité de formaliser un protocole pour la mise en œuvre d'audits internes dans un document interne, en définissant le champ d'application, la fréquence, les personnes responsables, les objectifs, la manière de les mettre en œuvre et d'en rendre compte, et les mesures requises en cas de traitement perçu comme étant illicite de données à caractère personnel.

Lors du contrôle, il s'est avéré que l'autorité responsable, aux fins de l'accès au système d'information qui permettait la traçabilité du traitement de données à caractère personnel, utilisait un système de noms d'utilisateurs et de mots de passe qui n'expiraient pas, et auquel tous les médecins et infirmiers avaient les mêmes droits d'accès. Un médecin pouvait consulter les données de tous les patients qui avaient été ou étaient encore traités au sein de l'autorité responsable. Par ailleurs, aucune exigence ne portait sur la complexité du mot de passe choisi, ce qui constitue un écart grave des bonnes pratiques acceptées dans le domaine de l'informatique et de la sécurité des informations. Considérant la nature des données à caractère personnel traitées par l'autorité responsable dans le système d'information et compte tenu des risques encourus, ces pratiques sont inacceptables. Par conséquent, le commissaire à l'information a ordonné à l'autorité d'inclure une politique sur les mots de passe dans un règlement interne et de procéder à sa mise en œuvre.

Pouvoirs de police dans le cas de l'accès aux données d'internautes

Le commissaire à l'information a reçu une plainte relative à l'utilisation des pouvoirs de police en lien avec l'acquisition de données d'utilisateurs de sites web dont le contenu est fourni par les bénéficiaires du service ou les utilisateurs (sites web tels que les forums en ligne, les sites web de médias, etc.). La plainte faisait état de suspicions que, dans un nombre inconnu de cas, des données à caractère personnel d'utilisateurs de forums en ligne avaient été obtenues en dehors de toute base juridique appropriée. Sur la base de l'analyse des données fournies par la police, le commissaire à l'information a noté que la police n'utilisait pas la législation correcte pour l'acquisition de données à caractère personnel de la part d'opérateurs de forums, qui sont des prestataires de services de la société de l'information (et non de la part d'opérateurs de réseaux de communications électroniques). La police s'appuyait en effet sur les dispositions de la loi de procédure pénale, de la loi sur la police, voire de la loi sur la protection des données à caractère personnel, plutôt que de la loi sur le marché du commerce

électronique, qui réglemente l'obtention d'informations de la part de prestataires de services de la société de l'information. Dans certains cas, aucune base juridique n'était indiquée. Il s'est également avéré que les différences entre les opérateurs (fournisseurs de services et de réseaux de communications électroniques accessibles au public) dont les opérations sont essentiellement régies par la loi sur les communications électroniques, et les opérateurs de sites web (prestataires de services de la société de l'information) dont les opérations relèvent principalement de la loi sur le marché du commerce électronique, n'étaient pas connues. Le commissaire à l'information a informé le ministère de l'intérieur et le bureau du procureur général de la République de Slovénie des conclusions du contrôle, et a suggéré la préparation d'un rapport y répondant, qui inclurait une liste de mesures destinées à résoudre les déficiences identifiées. Fin 2013, le commissaire à l'information a reçu un rapport intermédiaire de la part du ministère de l'intérieur. L'affaire était encore en cours de résolution en 2014.

Perte des signatures d'électeurs appelant à un référendum législatif

Suite aux rapports des médias sur les listes manquantes des signataires appelant à un référendum législatif sur la loi définissant les mesures prises par la République de Slovénie pour renforcer la stabilité bancaire, le commissaire à l'information a ouvert une procédure de contrôle d'office à l'Assemblée nationale et au ministère de l'intérieur, concernant la mise en œuvre des dispositions de la LPDP. Au cours de ce contrôle, il s'est avéré que le nombre de signatures ou de feuilles de papier de la liste d'initiateurs (c'est-à-dire, de signataires) n'avait pas été vérifié ou documenté de manière appropriée par l'Assemblée nationale lors de l'acceptation ou de la photocopie et de la communication de la liste au ministère de l'intérieur, et que l'authenticité des signatures n'avait pas non plus été vérifiée. Le ministère n'avait pas non plus bien documenté ni vérifié la taille réelle de la liste contenant des données à caractère personnel lors de la réception des photocopies, de leur distribution parmi les employés à des fins de vérification ou de leur retour suite à la vérification de la liste. Ce n'est qu'après l'intervention de l'initiateur en réponse au nombre apparemment insuffisant de signatures, qu'une vérification interne a été effectuée à l'Assemblée nationale et que les feuilles ont été comptées, établissant que la liste originale de signatures reçue se composait de 307 feuilles de papier, alors que le ministère de l'intérieur avait rendu les photocopies de 271 feuilles vérifiées. Il a par conséquent été établi qu'il manquait 36 feuilles photocopiées contenant les données à caractère personnel de 361 signataires. Le commissaire à l'information a établi que les autorités responsables avaient agi en violation des exigences de la LPDP sur les procédures et les mesures de protection des données à caractère personnel, et qu'elles n'avaient pas vérifié ni enregistré la taille et le contenu de la liste des signataires de l'initiative des électeurs appelant à un référendum législatif. Les autorités n'avaient par ailleurs pas assuré la traçabilité externe et ne s'étaient pas assurées qu'il serait possible d'établir ultérieurement quelles données à caractère personnel des signataires de l'initiative avaient ou n'avaient pas été remises à l'autre autorité responsable. En raison des irrégularités identifiées, le commissaire à l'information a imposé une sanction à l'encontre des personnes responsables à l'Assemblée nationale et au ministère de l'intérieur.

Destruction prématurée de dossiers médicaux

Suite à une plainte, le commissaire à l'information a ouvert une procédure de contrôle à l'encontre d'une entité responsable (une station thermale) en raison de la prétendue destruction illicite du dossier médical d'une personne trois ans à peine après la fin de son traitement. Il a été établi pendant le contrôle que le règlement interne de l'entité responsable fixait différentes périodes de conservation (5 à 15 ans) pour les données à caractère personnel des patients. Malgré ces périodes de conservation, l'entité responsable, en raison de possibilités techniques et d'espace de stockage limités face aux grandes quantités de dossiers médicaux au format papier, ne conservait les dossiers médicaux que trois ans après la fin du traitement au sein de la station thermale. Les dossiers médicaux destinés à être détruits étaient pesés, mais aucune liste des noms des patients dont les dossiers étaient détruits, n'était produite en raison du très grand nombre de dossiers (2 500 à 3 000 environ). Le commissaire à l'information a observé que les stations thermales étaient, conformément à la législation pertinente, considérées comme des prestataires de soins, et qu'elles devaient par conséquent respecter les

dispositions d'une loi spéciale, la ZZPPZ, en matière de stockage de données à caractère personnel. En vertu de la ZZPPZ, les dossiers et les antécédents cliniques des patients doivent être conservés 10 ans après le décès du patient, les autres documents médicaux de base devant être conservés pendant 15 ans. Le commissaire à l'information a également reçu un avis du ministère de la santé selon lequel les documents médicaux générés dans les stations thermales devaient être considérés comme faisant partie du dossier médical et des antécédents cliniques du patient, et qu'il convenait de les conserver 10 ans après le décès du patient. Le commissaire à l'information a ordonné à l'entité responsable de s'assurer que les données à caractère personnel des utilisateurs de leurs services de santé soient stockées et détruites conformément aux dispositions de la ZZPPZ, c'est-à-dire 10 ans après le décès de l'utilisateur. Il a également été ordonné à l'entité de s'assurer de la traçabilité, de manière à ce que la date de chaque destruction et que les personnes dont les données ont été détruites (nom, prénom et numéro de dossier du patient) puissent clairement être déterminées. Les problèmes de manque d'espace et de traçabilité peuvent être aisément résolus en stockant les données sous un format électronique, la ZZPPZ ne précisant pas sous quel format les prestataires de soins doivent stocker les dossiers contenant des données à caractère personnel.

Publication de données à caractère personnel de clients sur l'écran d'accueil d'un réparateur

Le commissaire à l'information a été informé qu'un atelier de réparation de véhicules (l'entité responsable) utilisait un système de réservation électronique et que les données à caractère personnel du client suivant apparaissaient sur son écran d'accueil : nom et prénom du client, heure d'admission, marque et numéro d'immatriculation de son véhicule, et nom et prénom du conseiller du client. D'après l'organisation, les écrans susmentionnés avaient pour but d'informer les clients du moment où leurs véhicules seraient acceptés et quel conseiller ils devaient contacter. Les clients avaient été satisfaits de l'introduction de cet écran, de sorte que, de l'avis de l'organisation, son utilisation représentait une mesure organisationnelle nécessaire qui permettait aux clients de gagner du temps et de l'argent, et aux techniciens de mieux préparer leur travail et donc, d'améliorer la qualité de service. Le commissaire à l'information a souligné qu'une technologie intégrant le traitement de données à caractère personnel devait également être considérée du point de vue de la finalité de son utilisation. Si le but du responsable du traitement des données est de traiter les données à caractère personnel de personnes (nom, prénom et numéro d'immatriculation du véhicule du client), alors, par sa nature même, il s'agit d'un traitement de données à caractère personnel qui doit reposer sur une base juridique appropriée. La publication de données à caractère personnel sur un écran d'accueil représente la communication, la diffusion et la mise à disposition de données à caractère personnel pour quiconque se trouve dans les locaux du réparateur au moment de leur publication. Ce type de traitement n'est certainement pas nécessaire ni approprié pour le respect des obligations, contractuelles ou autres, de l'entité responsable ni pour les intérêts légitimes d'une entreprise du secteur privé, ce qui signifie que l'entité responsable ne bénéficiait d'aucune base juridique pour y procéder. L'organisation ne disposait par ailleurs pas du consentement personnel des personnes pour procéder à ce traitement. Le commissaire à l'information a ordonné à l'entité responsable de mettre un terme à la publication des données à caractère personnel de ses clients/parties contractantes (nom, prénom et numéro d'immatriculation du véhicule du client) sur l'écran d'accueil de ses unités de service ou d'obtenir le consentement personnel explicite de chaque client avant de traiter leurs données.

C. Autres informations importantes

Les employés du commissaire à l'information participent régulièrement à des conférences et séminaires internationaux où ils présentent souvent leur propre travail.

En tant qu'autorité nationale de contrôle de la protection des données à caractère personnel, le commissaire à l'information coopère avec les instances compétentes de l'Union européenne (UE) et du Conseil de l'Europe concernées par la protection des données à caractère personnel.

En raison de coupes budgétaires, le commissaire à l'information n'a participé en 2013 qu'aux réunions plénières de l'Union européenne les plus urgentes et à quelques réunions de quatre des nombreux sous-groupes du groupe de travail « Article 29 ». Au total, le commissaire à l'information a participé à huit groupes de travail de l'UE engagés dans la supervision de la mise en œuvre de la protection des données à caractère personnel dans des domaines individuels de l'UE, à savoir :

- le groupe de travail « Article 29 » sur la protection des données à caractère personnel et quatre de ses sous-groupes (le sous-groupe Technologie, le sous-groupe Avenir de la protection de la vie privée, le sous-groupe Règles d'entreprise contraignantes (BCR) et le sous-groupe Frontières, déplacements et application de la loi (BTLE)) ;
- l'autorité de contrôle commune d'Europol ;
- l'autorité de contrôle commune de Schengen ;
- l'autorité de contrôle commune des douanes ;
- les réunions de coordination du Contrôleur européen de la protection des données (CEPD) et des autorités nationales de la protection des données à caractère personnel pour la supervision du SIS II ;
- les réunions de coordination du Contrôleur européen de la protection des données (CEPD) et des autorités nationales de la protection des données à caractère personnel pour la supervision du SID ;
- les réunions de coordination du Contrôleur européen de la protection des données (CEPD) et des autorités nationales de la protection des données à caractère personnel pour la supervision du VIS ;
- les réunions de coordination du Contrôleur européen de la protection des données (CEPD) et des autorités nationales de la protection des données à caractère personnel (EURODAC).

En mars 2013, le commissaire à l'information a été élu président de l'autorité de contrôle commune d'Europol. Le commissaire à l'information a également participé activement au groupe de travail international sur la protection des données dans les télécommunications (IWGDPT), qui rassemble des représentants des commissaires à l'information et des autorités de la protection des données à caractère personnel et de la vie privée du monde entier. Une fois encore en 2013, un représentant du commissaire à l'information a participé au comité consultatif (T-PD) du Conseil de l'Europe concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108).

Le 19 juillet 2013, la commissaire à l'information, Nataša Pirc Musar, a été désignée par la Commission européenne pour siéger dans un groupe ad hoc UE–États-Unis spécial, dont la tâche était de déterminer le niveau réel d'activité de la NSA, l'agence nationale de sécurité américaine, dans le cadre de la collecte massive d'informations et de données à caractère personnel de citoyens de l'Union européenne. Nataša Pirc Musar a participé à ce groupe spécial en tant que l'un des cinq grands experts européens dans le domaine de la protection des données à caractère personnel. À la fin de son mandat, le groupe a préparé un rapport sur ses conclusions, qu'il a remis à la Commission européenne.

Sur la base de l'article 60 de la décision 2007/533/JAI du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération et de l'article 44 du règlement (CE) nº 1987/2006 du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), le commissaire à l'information est chargé du contrôle indépendant de la licéité du traitement des données à caractère personnel SIS II sur son territoire et de leur transmission depuis son territoire. En 2013, le

commissaire à l'information n'a reçu aucune plainte concernant la mise en œuvre de ces droits en première instance.

En 2013, la République de Slovénie a mené une évaluation de la mise en œuvre des acquis de Schengen en termes de protection des données à caractère personnel, à laquelle le commissaire à l'information a activement participé.

En 2013, le commissaire à l'information a accueilli les représentants d'institutions similaires en Croatie, Bosnie-Herzégovine et Macédoine. Ils ont pris connaissance des opérations et des bonnes pratiques du commissaire dans les domaines dont il est responsable.

En 2013, le commissaire à l'information, en tant que partenaire chef de file, a réussi la mise en œuvre du projet de jumelage léger SR/2009/IB/JH/01 pour l'amélioration de la protection des données à caractère personnel en Serbie. Dans le contexte de la coopération internationale dans le domaine de l'accès aux informations publiques, en 2013, le commissaire à l'information a commencé à participer, pour une période de deux ans, à un consortium international au sein du projet LAPSI 2.0, qui a vocation à poursuivre le travail du projet LAPSI 1.0 et à établir un réseau thématique d'experts dans le domaine de la réutilisation des informations publiques, afin d'éliminer les obstacles à sa mise en œuvre que l'on peut observer dans la pratique.

Le 24 octobre 2013, le commissaire à l'information a organisé une conférence internationale sur le thème de la réutilisation des informations publiques. La conférence a été organisée dans le cadre du projet européen LAPSI (aspects juridiques des informations du secteur public, http://www.lapsi-project.eu/), qui a vocation à établir un réseau thématique d'experts dans le domaine de la réutilisation des informations publiques, est financé par la Commission européenne et auquel coopère le commissaire à l'information, en tant que l'un de ses partenaires. Cette conférence organisée à Ljubljana avait pour objet de présenter les nouveaux défis et tendances découlant de la modification de la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, en insistant particulièrement sur la question des données à caractère personnel. L'événement était également diffusé en direct sur Internet.

SUÈDE

A. Résumé des activités et actualités

L'attention apportée aux problèmes de protection des données par les médias, les responsables du traitement des données et le public s'est accrue en 2013. La *Datainspektionen* a gagné en visibilité dans les médias d'information et nous avons vu augmenter le nombre d'abonnés à nos communiqués de presse et à notre magazine. Nous avons organisé 62 séminaires et conférences dans l'année, ce qui représente une augmentation de 20 %. L'avis de notre DPA a été demandé sur un nombre croissant de propositions de nouvelles lois, pour un total de 116 avis. Notre travail a également gagné en importance sur le plan international. Les discussions sur la proposition de la Commission pour un nouveau règlement sur la protection des données se sont poursuivies, et notre DPA a suivi ce travail de près. La coopération entre les autorités de protection des données des États membres de l'UE s'est également poursuivie, et la DPA suédoise participe à plusieurs groupes de travail dans ce domaine.

L'entrée en vigueur de la nouvelle loi sur la vidéosurveillance le 1er juillet a été un événement important en 2013. Cette nouvelle loi donne à la *Datainspektionen* une responsabilité centrale pour le contrôle de la vidéosurveillance, et les compétences pour faire appel des décisions des conseils administratifs des comtés autorisant ce type de surveillance. La *Datainspektionen* y a consacré beaucoup de ressources et, au second semestre de 2013, quatre employés travaillaient à plein temps sur les questions liées à la vidéosurveillance.

Les révélations d'Edward Snowden sur la surveillance des communications sur Internet par la NSA ont été l'un des grands sujets de débats en Suède et dans d'autres pays en 2013. Des allégations selon lesquelles la police suédoise conservait des dossiers sur des personnes d'origine rom ont également entraîné un grand débat et ont donné lieu à un contrôle de terrain par le conseil de surveillance spécifique à la police.

Dans le cadre de nos activités de contrôle, le traitement de données à caractère personnel par les autorités publiques a été l'un de nos sujets de prédilection. Ce travail a porté, notamment, sur la supervision de l'échange d'informations entre autorités, l'utilisation de dispositifs mobiles et de services en nuage par les autorités publiques, ainsi que sur les développements liés à l'administration en ligne. La police a été un autre de nos chantiers, pour lequel nous avons collecté des informations sur leur traitement des données à caractère personnel en envoyant des questionnaires aux 21 autorités régionales de la police. Nous avons aussi effectué des contrôles de terrain auprès de ces autorités régionales. Enfin, nous avons effectué, pour la première fois, un contrôle auprès des services de renseignement militaires concernant leurs activités de traitement de données à caractère personnel.

Organisation	Conseil de l'inspection des données
Président et/ou collège	Mme Kristina Svahn Starrsjö, directrice générale
Budget	42 583 000 SEK = 4 288 750 €
Personnel	Environ 45 employés (= 41 équivalents temps plein)
Activités générales	
Décisions, avis, recommandations	26 décisions d'autoriser le traitement de données concernant des condamnations pénales (concernant pour la plupart les listes de l'OFAC) 64 avis en consultation avec des fonctionnaires chargés de la

	protection des données 214 décisions dans le cadre de contrôles (voir ci-dessous) 2 listes de vérification ; traitement de données à caractère personnel dans les bases de données de recrutement et activités de recherche
Notifications	3 378
Contrôles préalables	44 (concernant le traitement de données à caractère personnel dans les activités de recherche)
Demandes émanant de personnes concernées	230 demandes formelles, 6 100 questions par courriel, 7 100 appels téléphoniques
Plaintes émanant de personnes concernées	352
Conseils sollicités par le Parlement ou le gouvernement	116 demandes formelles, environ 70 consultations informelles
Autres renseignements relatifs aux activités générales	53 communiqués de presse, 62 exposés et séminaires
Activités d'inspection	
Contrôles, enquêtes	214
Activités de sanction	
Sanctions	---
Amendes	---
DPD	
Chiffres relatifs aux DPD	7 047 responsables du traitement ont désigné des DPD

B. Informations sur la jurisprudence

En mars 2013, le tribunal administratif du comté de Stockholm a rejeté l'appel d'une société de sécurité qui souhaitait créer une base de données, une sorte de « liste noire », afin d'empêcher les gens de quitter les stations essence sans payer leur carburant. La *Datainspektionen* a décidé en 2011 qu'une base de données de ce type ne saurait être autorisée en raison du volume de données à enregistrer, du risque d'informations incorrectes et de l'absence de moyens de rectifier les informations. Le tribunal administratif du comté a confirmé cette décision.

Dans le domaine des informations en matière de crédit, le tribunal administratif du comté a convenu, conformément à la précédente décision de la *Datainspektionen*, de requérir une autorisation formelle pour les abonnés qui avaient accès à des informations en matière de crédit sur Internet. Deux entreprises d'information en matière de crédit ont divulgué des informations sur Internet et demandé l'utilisation de noms d'utilisateurs et de mots de passe pour en permettre l'accès. La *Datainspektionen*

et le tribunal administratif du comté ont déclaré que ce type de divulgation requérait une autorisation plus formelle, telle que l'utilisation d'un identifiant électronique ou de mots de passe non réutilisables.

Une autre affaire judiciaire concernant les informations en matière de crédit portait sur l'obligation de fournir une copie des informations divulguées à la personne à laquelle ces informations faisaient référence. Lors de la divulgation d'informations en matière de crédit sur Internet, les sociétés ne fournissaient qu'un lien vers un site web où ces informations pouvaient être consultées. Dans sa décision, la *Datainspektionen* a déclaré que cette procédure n'était adéquate que si elle était optionnelle et si la personne l'acceptait et que, dans les autres cas, une copie papier devait être envoyée par courrier. Le tribunal administratif du comté a confirmé cet avis.

C. Autres informations importantes

Début 2013, la *Datainspektionen* a émis un avis sur un rapport d'une commission d'enquête qui s'était penchée sur la nécessité d'examiner les dispositions constitutionnelles sur la liberté d'expression. Dans cet avis, la DPA suédoise a suggéré l'introduction d'une disposition générale destinée à criminaliser plusieurs infractions du respect de la vie privée sur Internet. Nous recevons de nombreuses plaintes de personnes qui estiment que leur vie privée a été violée en raison de publications sur Internet. Dans de nombreux cas, nous ne pouvons pas agir parce que ces publications sont exonérées de la loi sur la protection des données à des fins de liberté d'expression. Dans notre avis, nous avons exprimé l'opinion qu'une disposition contenant des sanctions pénales pour de graves violations de la vie privée sur des sites web, etc. contribuerait à la prévention de ce type de comportements. Au cours de l'année, nous avons fourni aux enseignants des informations sur les droits et obligations de chacun sur Internet, afin qu'ils les transmettent à leurs élèves. Nous avons également organisé des séminaires pour la police et les procureurs afin de les aider dans leurs enquêtes sur les violations graves de la vie privée sur Internet.

En novembre 2013, la *Datainspektionen* a célébré son 40e anniversaire. La DPA suédoise a été créée en 1973 et a été la première autorité nationale de protection des données au monde.

Chapitre Trois
Union européenne et activités communautaires

3.1. Parlement européen

3.1.1 Projets de rapports de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) – 10 janvier 2013

La commission LIBE a présenté deux projets de rapports sur la réforme des règles de protection des données de l'UE, proposée par la Commission européenne. Jan-Philipp Albrecht, rapporteur de la proposition de règlement concernant la protection des données pour la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen, et Dimitrios Droutsas, rapporteur de la proposition de directive sur la protection des données pour les services répressifs, ont pleinement apporté leur soutien à un cadre de protection des données cohérent et robuste prévoyant des droits solides et exécutoires pour les personnes, et ont souligné le besoin d'un haut niveau de protection pour toutes les activités de traitement de données au sein de l'Union européenne afin de renforcer la certitude, la clarté et la cohérence juridiques.

Les points clés comprennent le remplacement de la directive 95/46/CE par un règlement directement applicable couvrant le traitement des données à caractère personnel par les secteurs privé et public, comprenant un seul ensemble de règles valides à travers l'UE, le soutien en faveur d'un « guichet unique » pour les sociétés qui déploient leurs activités dans plusieurs pays de l'UE et pour les consommateurs souhaitant porter plainte contre une société établie dans un autre pays que le leur, et une agence européenne de la protection des données puissante et indépendante chargée de prendre des décisions juridiquement contraignantes vis-à-vis des autorités nationales de protection des données ; le soutien en faveur du renforcement des droits des utilisateurs ; et l'applicabilité des règles européennes qui régissent le traitement des données à caractère personnel des citoyens européens à l'étranger par des sociétés qui ne sont pas établies au sein de l'UE.

3.1.2 Rapport de la commission de l'industrie, de la recherche et de l'énergie (ITRE) – 20 février 2013

La commission ITRE a adopté son avis sur les propositions de la Commission de réformer les règles de protection des données européennes. Cet avis sera transmis à la commission des libertés civiles, de la justice et des affaires intérieures (LIBE), qui consolidera l'ensemble des modifications soumises jusqu'ici et votera son propre rapport à la fin du mois d'avril.

La commission ITRE a appuyé les principales innovations de la réforme de la protection des données par la Commission. L'avis de la commission ITRE a fait suite à la publication, le 10 janvier 2013, des projets de rapports de la commission LIBE sur la réforme des règles de protection des données de l'UE.

3.1.3 Avis de la commission des affaires juridiques (JURI) – 19 mars 2013

La commission JURI a adopté ses avis sur les propositions de la Commission de réformer les règles de protection des données de l'UE. Ces avis seront soumis à la commission des libertés civiles, de la justice et des affaires intérieures (LIBE).

La commission JURI a appuyé l'architecture et les principes fondamentaux de la réforme de la protection des données par la Commission :

Les avis de la commission JURI font suite à la publication des projets de rapports sur la réforme des règles de protection des données de l'UE par la commission LIBE le 10 janvier 2013 et aux votes des commissions ITRE, EMPL et IMCO.

3.1.4 Rapports de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) – 22 octobre 2013

La commission LIBE a adopté deux rapports sur la réforme des règles de protection des données de l'UE proposée par la Commission européenne, et apporté son soutien à l'architecture et aux principes fondamentaux des propositions de réforme de la protection des données par la Commission, concernant le règlement général sur la protection des données et la directive sur la protection des données pour les services répressifs.

Le vote de la commission LIBE donne mandat aux rapporteurs, les députés européens Albrecht et Droutsas, pour négocier avec le Conseil de l'UE.

3.2. Commission européenne

Le 27 novembre 2013, la Commission européenne a présenté un ensemble de mesures à prendre pour restaurer la confiance dans les flux de données entre l'UE et les États-Unis suite aux inquiétudes soulevées par les révélations sur les programmes de collecte de renseignements à grande échelle des États-Unis, qui ont eu un impact négatif sur les relations transatlantiques.

Cet ensemble se composait d'un document stratégique prenant la forme d'une communication sur les flux transatlantiques de données, qui définit les défis et les risques suite aux révélations sur les programmes de collecte de renseignements des États-Unis, ainsi que les mesures qu'il convient de mettre en œuvre pour résoudre ces problèmes ; d'une analyse du fonctionnement de la sphère de sécurité, qui réglemente les transferts de données à des fins commerciales entre l'UE et les États-Unis ; d'un rapport factuel sur les conclusions du groupe de travail UE-États-Unis sur la protection des données, mis en place en juillet 2013 ; d'un examen des accords existants sur les dossiers passagers (PNR) ; et d'un examen du programme de surveillance du financement du terrorisme (TFTP), qui réglemente les échanges de données dans ces secteurs à des fins répressives.

La Commission a appelé à l'adoption rapide de la réforme de la protection des données ; au renforcement de la sécurité de la sphère de sécurité ; au renforcement des garanties de protection des données dans le domaine des services répressifs ; à l'utilisation des accords d'assistance juridique mutuelle et sectoriels existants pour obtenir des données ; à la réponse aux préoccupations européennes concernant le processus de réforme en cours aux États-Unis ; et à la promotion de normes internationales de respect de la vie privée.

3.2.1 Reconstruire la confiance dans les flux de données entre l'UE et les États-Unis

La communication définit six domaines où des mesures sont requises :

Une adoption rapide de la réforme européenne de la protection des données : le solide cadre législatif, tel que proposé par la Commission européenne en janvier 2012, avec des règles claires également applicables dans les situations où les données sont transférées et traitées à l'étranger, est une nécessité aujourd'hui plus que jamais. Les institutions européennes devraient dès lors continuer à travailler à l'adoption de la réforme européenne de la protection des données jusqu'au printemps 2014 afin de s'assurer que les données à caractère personnel sont protégées de manière efficace et exhaustive.

Renforcement de la sécurité de la sphère de sécurité : la Commission a émis aujourd'hui 13 recommandations en faveur de l'amélioration du fonctionnement du système de la sphère de sécurité après qu'une analyse également publiée aujourd'hui a conclu que le fonctionnement du système était déficient à plusieurs égards. Des recours devraient être identifiés avant l'été 2014. La Commission examinera alors le fonctionnement du système sur la base de la mise en œuvre de ces 13 recommandations.

Renforcement des garanties de protection des données dans le domaine des services répressifs : les négociations actuelles sur un « accord-cadre » pour les transferts et le traitement de données dans le contexte de la coopération avec les services policiers et judiciaires devraient être conclues rapidement. Cet accord doit garantir un haut niveau de protection pour les citoyens qui devraient bénéficier des mêmes droits des deux côtés de l'Océan Atlantique. Les citoyens européens qui ne résident pas aux États-Unis devraient notamment bénéficier de mécanismes de recours judiciaire.

Utilisation des accords d'assistance juridique mutuelle et sectoriels existants pour obtenir des données : En règle générale, l'administration américaine devrait s'engager à utiliser un cadre juridique, tel que les accords d'assistance juridique mutuelle et sectoriels entre l'UE et les États-Unis que sont l'accord relatif aux dossiers passagers et le programme de surveillance du financement du terrorisme, dès lors que des

transferts de données sont nécessaires à des fins répressives. Demander directement aux entreprises ne devrait être possible que dans des situations clairement définies, exceptionnelles et justiciables.

Réponse aux préoccupations européennes concernant le processus de réforme en cours aux États-Unis : Le Président américain Barack Obama a annoncé un examen des activités des autorités nationales de sécurité américaines. Ce processus devrait également bénéficier aux citoyens européens. Les changements les plus importants devraient porter sur l'extension des garanties à disposition des citoyens américains aux citoyens européens qui ne résident pas aux États-Unis, une plus grande transparence et une meilleure supervision.

Promotion de normes internationales de respect de la vie privée : Les États-Unis devraient pouvoir participer à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) du Conseil de l'Europe, de la même manière qu'ils ont participé à la Convention sur la cybercriminalité en 2001.

La Commission a également établi de manière très claire que les normes de protection des données ne feront pas partie des négociations en cours sur un partenariat transatlantique de commerce et d'investissement.

3.2.2 Rapport sur les conclusions du groupe de travail ad hoc UE-États-Unis sur la protection des données

Ce rapport a fait suite aux révélations relatives à l'existence de plusieurs programmes de surveillance américains reposant sur la collecte et le traitement à grande échelle de données à caractère personnel par des fournisseurs de services Internet et de télécommunications américains, et la surveillance des flux de données aux États-Unis et en dehors, ce qui peut avoir un impact important sur les citoyens européens.

Des clarifications ont été demandées aux autorités américaines sur plusieurs aspects, tels que l'étendue des programmes, les volumes de données collectées, l'existence de mécanismes de supervision judiciaire et administrative et leur disponibilité vis-à-vis des citoyens européens, ainsi que les différents niveaux de protection et de garantie procédurale applicables aux citoyens américains et européens. Un groupe de travail ad hoc UE-États-Unis a par la suite été établi afin d'établir les faits relatifs aux programmes de surveillance américains et à leur impact sur les droits fondamentaux au sein de l'Union européenne et sur les données à caractère personnel des citoyens européens.

Les États-Unis ont fourni des informations sur la base juridique sur laquelle reposent ces programmes de surveillance, et expliqué que l'autorité du président en matière de collecte de renseignements extérieurs en dehors des États-Unis, découlait directement de ses capacités de commandant en chef, ainsi que de ses compétences en matière de politique étrangère telles que prévues par la constitution américaine.

Le rapport a conclu que, en vertu du droit américain, plusieurs bases juridiques autorisaient la collecte et le traitement à grande échelle de données à caractère personnel transférées vers les États-Unis ou traitées par des entreprises américaines, à des fins de renseignement extérieur, telles que la lutte contre le terrorisme. Les États-Unis ont confirmé l'existence et les principaux éléments de certains aspects de ces programmes en vertu desquels avaient lieu la collecte et le traitement de données en lien avec le droit américain qui fixe des garanties et conditions spécifiques. Le nombre de citoyens européens affectés par ces programmes de surveillance et l'étendue géographique de ces programmes n'ont pas clairement été établis.

Les garanties applicables aux personnes concernées au sein de l'Union européenne et aux personnes concernées aux États-Unis présentent des différences, puisque la collecte de données de citoyens américains n'est en général pas autorisée. En cas d'autorisation, ces données ne sont alors considérées comme des « renseignements extérieurs » qu'en cas de nécessité par rapport aux fins spécifiées. Cette exigence de nécessité ne s'applique pas aux données des citoyens européens, qui sont considérées

comme des « renseignements extérieurs » si elles ont trait aux fins poursuivies. Il en résulte l'application de seuils moins élevés pour la collecte des données à caractère personnel des citoyens européens.

Les procédures de ciblage et de minimisation visent à réduire la collecte, la conservation et la diffusion de données à caractère personnel de, ou concernant des citoyens américains, et n'imposent pas d'exigences ou de restrictions spécifiques en matière de collecte, de traitement ou de conservation de données à caractère personnel des citoyens européens. La supervision des programmes de surveillance a principalement vocation à protéger les citoyens américains. Les citoyens américains bénéficient de protections constitutionnelles (les premier et quatrième amendements respectivement) qui ne s'appliquent pas aux citoyens européens ne résidant pas aux États-Unis.

Les différents niveaux de garantie de protection des données s'appliquent à différents types de données (métadonnées contre données de contenu) et à différents stades du traitement de données (acquisition initiale contre traitement/analyse ultérieur). L'utilisation d'autres bases juridiques et l'existence d'autres programmes de surveillance n'ont pas clairement été établies.

Les ordonnances pertinentes du FISC étant classifiées et les sociétés tenues de garder le secret quant à l'assistance qui leur est demandée, les personnes concernées au sein de l'Union européenne ou aux États-Unis n'ont aucun recours, judiciaire ou administratif, pour être informées de la collecte ou du traitement ultérieur de leurs données à caractère personnel. Les personnes ne bénéficient d'aucune opportunité ni d'aucun recours administratif ou judiciaire pour obtenir l'accès à, rectifier ou effacer des données.

Il existe une forme de supervision judiciaire des activités qui impliquent une exigence de divulgation d'informations. Il n'existe aucune forme d'autorisation judiciaire de sélecteurs individuels permettant de consulter les données collectées ou de demander qui est chargé de cette collecte. Il n'existe aucune supervision judiciaire de la collecte de renseignements extérieurs en dehors des États-Unis, qui est effectuée en vertu de la compétence exclusive du pouvoir exécutif.

3.2.3 Communication relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union européenne et des entreprises établies sur son territoire

En 2000, la Commission a adopté la décision 520/2000/CE, reconnaissant les principes de la sphère de sécurité et les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, comme assurant un niveau de protection adéquat aux fins des transferts de données à caractère personnel depuis l'UE vers les États-Unis.

La décision relative à la sphère de sécurité permet donc le transfert d'informations personnelles depuis l'UE vers des entreprises établies aux États-Unis qui se sont engagées à respecter les principes de respect de la vie privée, dans les cas où le transfert ne satisferait pas autrement aux exigences de l'UE en matière d'adéquation du niveau de protection des données à caractère personnel. Le fonctionnement de l'accord sur la sphère de sécurité repose sur les engagements pris par les entreprises membres et l'autocertification de celles-ci. La signature revêt un caractère volontaire, mais les règles sont contraignantes pour les signataires. Les principes fondamentaux de cet accord sont la transparence des politiques de protection de la vie privée adoptées par les entreprises, l'intégration des principes de la sphère de sécurité dans les politiques de protection de la vie privée adoptées par les entreprises, et la mise en œuvre, y compris par les autorités publiques.

La sphère de sécurité doit être réexaminée en raison de la croissance exponentielle des flux de données, de la rapide croissance de l'économie numérique et des grandes évolutions en matière de collecte, de traitement et d'utilisation des données ; de l'importance des flux de données, notamment pour l'économie transatlantique ; de l'augmentation du nombre d'entreprises rejoignant la sphère de sécurité (multiplié par huit depuis 2004) ; et des informations récemment diffusées sur les programmes de surveillance américains, qui soulèvent de nouvelles questions quant au niveau de protection que l'accord sur la sphère de sécurité est censé garantir.

La Communication est fondée sur des éléments recueillis par la Commission, les travaux du groupe de contact UE/États-Unis sur la protection de la vie privée menés en 2009, une étude réalisée en 2008 par un contractant indépendant et les informations reçues par le groupe de travail ad hoc UE/États-Unis, créé à la suite des révélations sur les programmes de surveillance américains. Elle fait suite aux rapports d'évaluation de la Commission de 2002 et 2004.

La Communication reconnait que la sphère de sécurité a été un vecteur pour les flux de données à caractère personnel entre l'Union européenne et les États-Unis, que les entreprises américaines ont des centaines de millions de clients dans l'UE, et que le volume des transferts relève d'une échelle inconcevable en premier lieu.

Les sujets requérant l'attention comprennent la transparence des dispositions de protection de la vie privée adoptées par les adhérents à la sphère de sécurité, la mise en œuvre effective des principes relatifs à la protection de la vie privée par les entreprises établies aux États-Unis, et le caractère effectif du contrôle de l'application desdits principes. L'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis soulève des questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis.

La Commission a dès lors formulé les recommandations suivantes, en matière de transparence :

- les entreprises autocertifiées devraient rendre publiques leurs dispositions de protection de la vie privée. ;

- les dispositions de protection de la vie privée rendues publiques sur les sites web respectifs des entreprises autocertifiées devraient toujours inclure un lien pointant vers le site web du ministère du commerce consacré à la sphère de sécurité, qui dresse la liste de l'ensemble des adhérents au cadre dont la certification est à jour ;

- les entreprises autocertifiées devraient publier les conditions de protection de la vie privée figurant dans tout contrat conclu entre elles et leurs sous-traitants, par exemple, pour les services d'informatique en nuage ;

- le site web du ministère du commerce devrait clairement signaler toutes les entreprises dont la certification n'est plus à jour.

En matière de recours, la Commission formule les recommandations suivantes :

- les dispositions de protection de la vie privée mises sur les sites web des entreprises doivent inclure un lien dirigeant vers le site d'un prestataire de règlement extrajudiciaire des litiges (REL) et/ou du panel de l'UE sur la protection des données ;

- le REL devrait être facilement accessible et abordable économiquement ;

- le ministère du commerce devrait contrôler plus systématiquement les prestataires de REL sous l'angle de la transparence et de l'accessibilité des informations qu'ils fournissent à propos des procédures utilisées et du suivi accordé aux plaintes.

Concernant la mise en œuvre, la Commission formule les recommandations suivantes :

- à la suite d'une certification ou d'un renouvellement de la certification d'entreprises au titre de la sphère de sécurité, un certain pourcentage d'entre elles devraient être soumises à des enquêtes d'office concernant le respect effectif de leurs dispositions de protection de la vie privée (allant au-delà du contrôle du respect des exigences formelles) ;

- toutes les fois où une non-conformité est constatée, à l'issue d'une plainte ou d'une enquête, l'entreprise concernée devrait, après un an, faire l'objet d'une enquête de suivi spécifique ;

- en cas de doutes au sujet de la conformité d'une entreprise ou si des plaintes sont en cours d'examen, le ministère du commerce devrait en informer l'autorité compétente chargée de la protection des données dans l'État membre de l'UE concerné ;

- les fausses déclarations d'adhésion à la sphère de sécurité devraient continuer à être examinées.

En ce qui concerne l'accès par les autorités des États-Unis, la Commission formule les recommandations suivantes :

- les politiques de protection de la vie privée adoptées par les entreprises autocertifiées doivent comporter des informations sur la mesure dans laquelle la législation des États-Unis permet aux autorités publiques de collecter et de traiter des données transférées selon les principes de la sphère de sécurité ; et

- la dérogation pour raison de sécurité nationale prévue par la décision relative à la sphère de sécurité ne devrait être utilisée que dans la mesure où cela est strictement nécessaire et proportionné.

3.2.4 Rapport d'évaluation sur le programme de surveillance du financement du terrorisme (TFTP)

Dans ce rapport sur la valeur qu'apportent les données fournies par le TFTP aux enquêtes de contre-terrorisme, la Commission conclut que le TFTP a permis de recueillir des renseignements importants grâce auxquels il a été possible de détecter des complots terroristes et de remonter jusqu'à leurs auteurs. Ces informations ont été utilisées pour enquêter sur les attentats du marathon de Boston en avril 2013, sur les menaces terroristes durant les jeux olympiques de Londres et sur l'entraînement en Syrie de terroristes basés dans l'UE.

Les données du TFTP sont une source essentielle d'informations sur les réseaux de financement des organisations terroristes et elles aident à mettre au jour les nouvelles méthodes de financement du terrorisme et à identifier les personnes impliquées, aux États-Unis, dans l'Union européenne ou ailleurs. Ces informations sont utiles aux États membres de l'UE et à Europol et leur procurent des pistes précieuses pour leurs enquêtes. Au cours des trois dernières années, en réponse à un total de 158 demandes soumises par les États membres et par l'UE, le TFTP a permis d'obtenir 924 pistes d'enquête.

En ce qui concerne les récentes allégations selon lesquelles les États-Unis auraient eu accès à des données de messagerie financière dans l'UE en violation de l'accord TFTP, le gouvernement américain a donné par écrit l'assurance qu'il n'avait pas enfreint l'accord et qu'il continuerait à le respecter intégralement. En 2013, il a été considéré qu'il n'était pas nécessaire de poursuivre les consultations avec les États-Unis sur l'application de l'accord TFTP.

En réponse aux demandes du Parlement européen et du Conseil, la Commission a également examiné les options envisageables en vue de la création d'un système européen de surveillance du financement du terrorisme (SSFT), en évaluant, pour chacune de ces options, le respect des droits fondamentaux, les critères de nécessité et de proportionnalité ainsi que le rapport coût/efficacité au regard de la situation actuelle.

La Commission est parvenue à la conclusion qu'il n'y avait pas d'intérêt de créer un système de ce type au sein de l'Union européenne, notamment car il serait nécessaire de créer et de gérer une base de données contenant toutes les informations relatives aux transferts financiers des citoyens de l'UE, et que la création d'une telle base de données comporterait des difficultés majeures en ce qui concerne le stockage des données, l'accès à ces dernières et leur protection, sans compter les besoins techniques et financiers considérables.

3.2.5 Rapport sur le réexamen conjoint de l'accord relatif aux dossiers passagers (PNR) entre l'UE et les États Unis

L'accord UE-États-Unis relatif au transfert des données des passagers aériens des vols en provenance de l'Union européenne à destination des États-Unis est entré en vigueur le 1er juillet 2012. À l'issue d'un contrôle réalisé par des experts de l'UE et des États-Unis, il s'est avéré que les autorités américaines avaient appliqué l'accord en respectant les normes et les conditions qu'il contient.

Cet accord fournit un outil efficace de lutte contre le terrorisme et les formes graves de criminalité transnationale, tout en limitant clairement les fins auxquelles les données PNR peuvent être utilisées et en apportant un ensemble de garanties solides en matière de protection des données.

Le rapport sur le réexamen conjoint conclut notamment que les autorités américaines respectent leurs obligations en ce qui concerne les droits d'accès des passagers et qu'elles ont mis en place un mécanisme de contrôle régulier pour se prémunir contre une discrimination illégale. Les obligations de masquage et de suppression des données sensibles sont respectées. Le partage de données avec les agences nationales américaines et avec les pays tiers est conforme aux termes de l'accord.

3.3. Cour de justice de l'Union européenne

3.3.1 Tribunal : T-214/11 - ClientEarth et PAN Europe contre EFSA (en appel)

Arrêt du Tribunal (sixième chambre) du 13 septembre 2013 – ClientEarth et Pesticide Action Network Europe (PAN Europe) contre Autorité européenne de sécurité des aliments (EFSA).

Dans cette affaire, la requérante a demandé à avoir accès, en vertu du règlement 1049/2001, à des documents préparés par des experts européens. La requérante connaissait les noms des experts, ainsi que le contenu des documents, mais souhaitait savoir quels experts étaient les auteurs des différents observations. La divulgation de ce type d'informations a été refusée sur la base du règlement 45/2001, qui prévoit que l'accès aux documents peut être refusé lorsque leur divulgation peut porter préjudice à la protection de la vie privée et à l'intégrité de la personne.

Les requérantes ont déclaré que l'institution en question avait divulgué sur son site web les noms, les biographies et déclarations d'intérêts de chacun des experts concernés, qui n'étaient dès lors pas des données à caractère personnel.

Le Tribunal a jugé que le fait que ces experts soient répertoriés sur un site Internet public n'impliquait pas nécessairement que leurs noms aient perdu leur nature de données à caractère personnel.

Ensuite, les requérantes ont fait valoir qu'un avis d'expert devait être divulgué même s'il pouvait être de nature à susciter des polémiques ou à dissuader la personne l'ayant formulé d'apporter sa contribution au processus décisionnel d'une institution.

Le Tribunal a jugé qu'il ne découlait pas de cela que le nom de tout expert ayant fait des observations sur un acte de l'Union ne pourrait pas être considéré comme une donnée à caractère personnel.

3.3.2 Cour de justice de l'Union européenne : C-486/12 – X

Arrêt de la Cour (huitième chambre) du 12 décembre 2013 dans la procédure engagée par X.

Dans cette décision, la Cour a jugé que l'article 12, sous a), de la directive 95/46 ne s'opposait pas à la perception de frais à l'occasion de la communication de données à caractère personnel par une autorité publique, dans la mesure où ces frais n'étaient pas excessifs. Les États membres peuvent fixer le montant desdits frais à un niveau qui constitue un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen de son droit de se voir communiquer les données sous une forme intelligible, afin de pouvoir, le cas échéant, exercer les droits de rectification, d'effacement et de verrouillage des données, en cas de non-conformité du traitement de celles-ci avec cette directive, ainsi que les droits d'opposition et d'introduction d'un recours juridictionnel et, d'autre part, la charge que l'obligation de communiquer ces informations représente pour le responsable du traitement.

Aux fins de l'article 12, sous a), lorsqu'une autorité publique nationale prélève des frais en contrepartie de l'exercice par une personne physique du droit d'accès aux données à caractère personnel la concernant, le montant de ces frais ne devrait pas excéder le coût de la communication de ces données. Une telle limite supérieure n'entrave toutefois pas la faculté, pour les États membres, de fixer à un niveau inférieur le montant desdits frais afin de garantir à toute personne physique que ledit droit d'accès demeure effectif.

3.3.3 Cour de justice de l'Union européenne : C-473/12 – IPI

Arrêt de la Cour (troisième chambre) du 7 novembre 2013 – Institut professionnel des agents immobiliers (IPI) contre Geoffrey Englebert et autres.

Dans cette décision, la cour a jugé que l'article 13, paragraphe 1, de la directive 95/46 devait être interprété en ce sens que les États membres ont non pas l'obligation, mais la faculté de transposer dans leur droit national une ou plusieurs des exceptions qu'il prévoit à l'obligation d'informer les personnes concernées du traitement de leurs données à caractère personnel, et que ses dispositions à cet égard sont assez générales et souples, laissant aux États membres le soin d'arrêter les détails.

Les États membres sont libres de décider si, et dans ce cas, à quelles fins, ils souhaitent inclure à leur droit des exceptions aux fins énumérées à cet article 13, paragraphe 1, sous a) à g), y compris des limitations de l'obligation d'information de la personne concernée. Ces mesures peuvent être prévues uniquement lorsqu'elles sont nécessaires.

La situation d'un détective privé engagé par un organisme professionnel afin de rechercher des manquements à la déontologie d'une profession réglementée est couverte par l'article 13, paragraphe 1, sous d). La directive 95/46 ne précisant pas les modalités de la recherche et de la détection des manquements à la réglementation, elle n'empêche pas un organisme professionnel d'avoir recours à des enquêteurs spécialisés pour accomplir sa mission.

Si le droit national le prévoit, ni l'organisme professionnel ni les détectives privés ne sont obligés d'informer la personne concernée, comme cela est prévu aux articles 10 et 11. Si le droit ne le spécifie pas, les personnes concernées doivent alors être informées.

Les États membres peuvent également estimer que les organismes professionnels et les détectives privés agissant pour le compte de ceux-ci sont capables d'accomplir leur mission sans se prévaloir des exceptions visées à l'article 13, paragraphe 1.

3.3.4 Cour de justice de l'Union européenne : C-342/12 – Worten

Arrêt de la Cour (troisième chambre) du 30 novembre 2013 – Worten - Equipamentos para o Lar SA contre Autoridade para as Condições de Trabalho (ACT).

Dans cette décision, la Cour a jugé que les articles 6, paragraphe 1, sous b) et c), ainsi que 7, sous c) et e), de la directive 95/46 ne s'opposaient pas à une réglementation nationale qui impose à l'employeur l'obligation de mettre à la disposition de l'autorité nationale compétente en matière de surveillance des conditions de travail le registre du temps de travail afin d'en permettre la consultation immédiate, pour autant que cette obligation est nécessaire aux fins de l'exercice par cette autorité de ses missions de surveillance de l'application de la réglementation en matière de conditions de travail, notamment, en ce qui concerne le temps de travail.

3.3.5 Cour de justice de l'Union européenne : C-291/12 – Schwarz

Arrêt de la Cour (quatrième chambre) du 17 octobre 2013 — Michael Schwarz contre Stadt Bochum.

Dans cette décision, la Cour a jugé que l'article 62, paragraphe 2, sous a), CE, qui faisait partie du titre IV du traité CE, habilitait le Conseil à réglementer le déroulement des contrôles effectués aux frontières extérieures de l'Union européenne et destinés à vérifier l'identité des personnes qui les franchissent. Une telle vérification impliquant nécessairement la présentation de documents qui permettent d'établir cette identité, l'article 62, paragraphe 2, sous a), CE autorisait par conséquent le Conseil à adopter des dispositions normatives relatives à de tels documents et, en particulier, aux passeports.

S'agissant de l'autorité du législateur européen dans ce domaine, la disposition (qui faisait référence aux contrôles de « personnes », sans davantage de précision) devait viser non seulement les ressortissants de pays tiers, mais aussi les citoyens de l'Union et, par conséquent, également les passeports de ces derniers.

D'autre part, l'harmonisation des normes de sécurité de ces passeports peut s'imposer en vue d'éviter que ces derniers ne présentent des dispositifs de sécurité moins perfectionnés que ceux prévus pour le modèle type de visa et pour le modèle uniforme de titre de séjour de ressortissants de pays tiers. Dans ces conditions, le législateur de l'Union doit être considéré comme étant compétent pour prévoir des éléments de sécurité équivalents pour les passeports des citoyens de l'Union, dans la mesure où une telle compétence permet d'éviter que ceux-ci deviennent la cible de falsifications et d'utilisations frauduleuses.

3.4. CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

A : Résumé des activités et actualités

Le Contrôleur européen de la protection des données (CEPD) est une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et la vie privée et de promouvoir les bonnes pratiques dans les institutions et organes de l'UE. À cet effet, il remplit les tâches suivantes :

- contrôler les traitements de données à caractère personnel effectués par l'administration de l'UE ;
- fournir des conseils sur les politiques et les textes législatifs qui touchent à la vie privée ; et
- coopérer avec des autorités de même nature afin de garantir une protection des données qui soit cohérente.

Dix ans après sa création, le CEPD a atteint sa maturité en tant qu'organisation et est en mesure de faire face aux nombreux défis qu'une autorité chargée de la protection des données doit relever dans un environnement très dynamique. Le principal défi opérationnel auquel nous avons été confrontés en 2013 a été de faire progresser le volume et la portée de nos activités malgré les contraintes budgétaires et les mesures liées aux ressources en raison de la crise financière.

Notre stratégie 2013-2014, ainsi que notre règlement intérieur et notre plan de gestion annuel, nous ont fourni des conseils précieux, exprimant la vision et la méthodologie requises pour améliorer notre capacité à travailler de manière efficace dans un climat d'austérité.

A.1. Activités de supervision et d'application

Nous avons observé une augmentation du nombre de notifications de contrôle préalable reçues dans le cadre de nos activités de supervision et de mise en application. Cette augmentation s'explique principalement par le délai, fixé à juin 2013, pour la soumission des notifications de contrôle préalable ex post concernant les opérations de traitement déjà en cours. La hausse du nombre d'avis émis durant l'année résulte également du nombre élevé de notifications reçues. Nous avons continué à assurer le suivi des recommandations formulées dans les avis antérieurs du CEPD relatifs aux contrôles préalables et avons pu clôturer un nombre considérable de cas.

Le nombre de réclamations reçues a diminué, ce qui est en partie dû à une meilleure information sur les compétences du CEPD et à une sensibilisation accrue à cet égard, mais également à l'efficacité de notre formulaire de réclamation en ligne.

Une des caractéristiques du plan d'action établi dans notre stratégie 2013-2014 consiste à promouvoir une « culture de protection des données » au sein des institutions et organes de l'UE de sorte qu'ils soient au fait de leurs obligations et assument la responsabilité du respect des exigences relatives à la protection des données.

À la lumière de ce qui précède, nous avons continué à fournir des orientations et des formations aux responsables du traitement, aux délégués à la protection des données (DPD) et aux coordinateurs de la protection des données (CPD), principalement sous la forme de lignes directrices en matière de marchés publics, de subventions et d'experts externes; de l'organisation d'une formation de base, destinée aux nouveaux DPD, sur la procédure de contrôle préalable ainsi que d'une formation spéciale destinée aux DPD de cinq entreprises communes de l'Union. Nos initiatives de sensibilisation dans les institutions et organes de l'Union européenne ont notamment consisté à organiser des ateliers spécifiques et généraux.

Un autre élément fondamental a été notre dialogue continu avec les responsables du traitement, les DPD et les CPD en vue de soutenir le travail des DPD. Ces réunions nous aident à mieux comprendre les contraintes rencontrées par les institutions en vue de leur donner des conseils concrets. De nombreuses réunions ont eu lieu avec des responsables du traitement, soit dans le cadre de contrôles préalables soit dans le cadre du suivi des avis et décisions. Les réunions du réseau des DPD, les réunions bilatérales et la ligne d'assistance pour les DPD ont constitué des instruments de communication utiles pour notre travail avec les DPD et les CPD.

A.2. Activités liées aux politiques et consultations

Tout au long de l'année 2013, nous sommes restés étroitement associés au travail en cours concernant la réforme du cadre européen relatif à la protection des données. Le 15 mars 2013, nous avons adressé au Parlement européen, à la Commission et au Conseil des observations supplémentaires au sujet de la réforme. Nous avons également continué de participer aux débats qui ont suivi, tant au Parlement qu'au Conseil.

En outre, la Commission a publié un grand nombre de propositions législatives ayant des incidences sur le droit fondamental à la protection des données à caractère personnel.

Nous avons abordé le sujet de la stratégie numérique et de l'internet à plusieurs reprises, notamment dans notre avis sur la communication de la Commission intitulée « Une stratégie numérique pour l'Europe – faire du numérique un moteur pour la croissance européenne », dans notre avis relatif au « Marché unique européen des communications électroniques » et dans notre avis sur le livre vert intitulé « Se préparer à un monde audiovisuel totalement convergent: croissance, création et valeurs ».

En ce qui concerne l'espace de liberté, de sécurité et de justice (ELSJ), nous avons émis des avis sur Europol, la stratégie de l'Union en matière de cybersécurité, les frontières intelligentes, les données des dossiers passagers (données PNR) UE-Canada ainsi que sur le modèle européen en matière d'échange d'informations.

Nos avis particulièrement importants concernant le marché intérieur ont été les suivants : avis sur la lutte contre le blanchiment de capitaux et le financement du terrorisme, les paiements au sein du marché intérieur, le droit européen des sociétés et la gouvernance d'entreprise et la facturation électronique dans le cadre des marchés publics.

Dans le domaine des services de santé en ligne, nous souhaitons attirer l'attention sur nos avis sur les dispositifs médicaux, sur les précurseurs de drogues et sur le plan d'action pour la santé en ligne.

A.3. Activités de coopération

Le CEPD coopère avec d'autres autorités chargée de la protection des données afin de promouvoir une protection des données cohérente à travers l'Europe. Cette fonction de coopération vise également la coopération avec des organes de contrôle relevant de l'ancien « troisième pilier » européen et dans le contexte des systèmes d'information à grande échelle.

En 2013, nous avons continué de contribuer activement aux activités du groupe de travail « Article 29 ». En particulier, nous avons fortement contribué, en tant que rapporteur ou co-rapporteur, aux avis relatifs à la limitation de la finalité et à l'intérêt légitime (sous-groupe « Dispositions-clés »), à l'avis sur le modèle d'analyse d'impact relative à la protection des données (sous-groupe « Technologie »), et à l'avis relatif aux données ouvertes (sous-groupe « Administration en ligne »).

La coopération directe avec les autorités nationales est de plus en plus importante dans le cadre du développement de bases de données internationales à grande échelle comme EURODAC, le système d'information sur les visas (VIS), le système d'information Schengen II (SIS II) et le système d'information douanier (SID), qui nécessitent une approche coordonnée de la supervision. En 2013, nous avons fourni

des services de secrétariat au nouveau groupe de coordination de la supervision de SIS II (SCG) et nous avons continué de présider les groupes de coordination d'EURODAC, VIS et du SID. Nous avons organisé deux réunions à Bruxelles pour chacun des groupes de coordination de supervision en 2013.

En outre, SIS II est devenu opérationnel. Afin de réduire les contraintes financières, administratives et en matière de déplacements, nous avons organisé des réunions consécutives des groupes de coordination de supervision et nous nous sommes efforcés d'établir des politiques de contrôle horizontales et cohérentes concernant les systèmes d'information à grande échelle, le cas échéant.

Le modèle des groupes de coordination de supervision sera élargi en 2014 par la création d'un groupe de coordination de supervision pour le système d'information du marché intérieur (IMI). En 2013, nous avons consulté les autorités nationales chargées de la protection des données (APD) et la Commission pour faire le point sur la situation et sur les évolutions du règlement IMI, afin d'organiser la première réunion du groupe en 2014.

Dans le cadre du Conseil de l'Europe, nous avons participé à trois réunions du comité consultatif de la Convention 108 du Conseil de l'Europe. Il était particulièrement important pour nous de participer à ces réunions afin de pouvoir suivre et influencer la modernisation en cours de la Convention.

Le CEPD a également participé aux travaux du groupe d'experts chargé de mettre à jour les lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) sur la protection de la vie privée.

Nous avons par ailleurs apporté une contribution significative aux questions liées à la protection des données dans plusieurs autres forums importants tels que la Coopération économique Asie-Pacifique (CEAP), l'Association francophone des autorités de protection des données personnelles (AFAPDP) et le groupe de travail international sur la protection des données dans les télécommunications (Groupe de Berlin).

Organisation	Contrôleur européen de la protection des données (CEPD)
Président et/ou collège	Peter Hustinx, contrôleur Giovanni Buttarelli, contrôleur adjoint
Budget	7 661 409 EUR
Personnel	62 (toutes catégories de personnel incluses)
Activités générales	
Décisions, avis, recommandations	20 avis législatifs portant, notamment, sur des initiatives liées à l'espace de liberté, de sécurité et de justice, à la stratégie numérique, aux services de santé en ligne, à la coopération internationale et au marché intérieur. 13 séries d'observations formelles concernant, notamment, 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 et le programme « Droits fondamentaux et citoyenneté ». 33 séries d'observations informelles

Notifications	272 notifications d'opérations de traitement reçues de la part de délégués à la protection des données auprès d'institutions et d'organes de l'UE à des fins de contrôles préalables
Contrôles préalables	91 avis de contrôle préalable adoptés concernant, notamment, la gestion des congés, l'évaluation du personnel, le recrutement, les suspicions et les délits, et les marchés publics. 21 avis sur l'absence de contrôle préalable adoptés
Demandes émanant de personnes concernées	176 demandes d'informations et de conseils de la part du public ou de parties intéressées, dont la majorité concernait l'obtention de plus d'informations sur des questions relatives à la protection de la vie privée ou demandant une assistance pour résoudre des problèmes, tels que la sécurité de leurs informations personnelles ou l'utilisation abusive de celles-ci.
Plaintes émanant de personnes concernées	78 plaintes reçues, dont 30 recevables
Conseils sollicités par le Parlement ou le gouvernement	La plupart des 20 avis législatifs susmentionnés ont été exprimés à la demande de la Commission européenne (article 28, paragraphe 2, du règlement (CE) nº 45/2001).
Autres renseignements relatifs aux activités générales	37 consultations reçues concernant des mesures administratives liées au traitement de données à caractère personnel dans l'administration de l'UE. Des conseils ont été donnés sur de nombreux aspects juridiques tels que les transferts de données relatives au personnel, le changement de finalité de la collecte de données à des fins spécifiques et les demandes d'accès public. Des lignes directrices ont été publiées sur le traitement de données à caractère personnel dans le domaine des marchés publics. Plusieurs ateliers et sessions de formation ont été organisés sur des sujets spécifiques tels que le rôle du DPD, des RH, des technologies de l'information et des marchés publics, et les procédures de notification et de contrôle préalable. Les ateliers ont couvert l'utilisation des communications électroniques et des appareils mobiles sur le lieu de travail, les sites web gérés par les institutions et organes de l'UE, et les flux de données transfrontaliers.
Activités d'inspection	
Contrôles, enquêtes	5 contrôles sur place et 2 visites réalisés.
Activités de sanction	S. o.
DPD	
Chiffres relatifs aux DPD	62 DPD au sein des institutions, organes et agences de l'UE.

B. Informations sur la jurisprudence

Affaires judiciaires

En 2013, le CEPD est intervenu dans plusieurs affaires portées devant la Cour de justice de l'Union européenne et le Tribunal de la fonction publique.

Le CEPD a présenté une plaidoirie lors d'une audience devant la grande chambre de la Cour de justice dans le cadre d'une procédure de renvoi préjudiciel. Cette audience concernait les affaires jointes : Digital Rights Ireland (C-293/12) et Seitlinger et autres (C-293/12). Ces deux affaires portent sur la validité de la directive 2006/24/CE sur la conservation des données.

C'est la première fois que la Cour invitait le CEPD à comparaître à une audience dans le cadre d'une procédure de renvoi préjudiciel. Pour le CEPD, il s'agissait d'une étape importante susceptible d'aboutir à une décision historique sur une question que nous suivons attentivement depuis plusieurs années.

Le CEPD a plaidé dans l'affaire Commission c. Hongrie (C-288/12). Cette affaire est la troisième procédure d'infraction relative à l'indépendance des autorités chargées de la protection des données, les deux autres étant les affaires Commission c. Autriche (C-614/10) et Commission c. Allemagne (C-518/07) dans lesquelles des arrêts ont respectivement été rendus en 2012 et en 2010.

D'autres affaires dans lesquelles le CEPD est intervenu sont toujours en instance, notamment Pachtitis c. Commission et EPSO (T-374/07), Pachtitis c. Commission (F-35/08), ZZ c. BEI (affaire F-103/11) ainsi que Dennekamp c. Parlement européen (T-115/13).

En octobre 2013, le CEPD a demandé le droit d'intervenir dans deux autres affaires : Elmaghraby et El Gazaerly c. Conseil de l'Union européenne (affaire T-319/13) et CN c. Parlement (affaire T-343/13).

C. Autres informations importantes

Révision du cadre européen en matière de protection des données

À la suite des nombreuses activités entreprises dans le cadre de la réforme en 2012 et de notre avis du 7 mars 2012, nous avons adressé des observations supplémentaires au Parlement européen, à la Commission et au Conseil le 15 mars 2013. Ces observations portaient sur des points particuliers nécessitant des éclaircissements et répondaient également aux amendements proposés par les commissions compétentes du Parlement européen.

Dans nos commentaires, nous avons également déconseillé d'exclure des secteurs spécifiques de la portée de l'application du cadre européen en matière de protection des données ; nous avons par ailleurs déconseillé de limiter la portée territoriale du règlement général proposé en matière de protection des données. Nous avons également réitéré que les données pseudonymisées restent des données à caractère personnel (ou des informations personnelles) et doivent être protégées en tant que telles. Toute définition des données anonymes ou des données pseudonymisées doit, dès lors, être pleinement cohérente avec la définition des données à caractère personnel et ne doit pas engendrer la suppression excessive de certaines catégories de données à caractère personnel de la portée du cadre en matière de protection des données. Nous avons soutenu l'élimination d'un éventuel traitement ultérieur des données en vue de finalités incompatibles et nous avons souligné que la définition du consentement explicite doit être conservée. Nous avons également apporté notre soutien à la définition relative aux responsables du traitement et aux sous-traitants et à leurs responsabilités telle que proposée par la Commission, ainsi qu'au principe de responsabilité qui doit s'appliquer à l'ensemble de la proposition. Certains éléments de l'approche dite fondée sur le risque étaient les bienvenus, mais nous avons indiqué que la protection complète telle que prévue dans le règlement doit s'appliquer à tous les traitements. En ce qui concerne les transferts internationaux, nous avons recommandé de clarifier les règles et nous avons accueilli

favorablement les amendements introduisant un nouvel article sur les transferts non autorisés en vertu de la législation européenne.

Pour ce qui est de la proposition de directive sur la protection des données en matière d'application de la législation pénale, nous avons apporté notre soutien à l'alignement le plus étroit de la proposition de directive sur la proposition de règlement et ce afin de veiller à la cohérence. Nous avons également accueilli favorablement les amendements introduisant des conditions et protections spécifiques en ce qui concerne l'accès par les autorités répressives aux données initialement traitées à d'autres fins et nous avons mis en évidence le fait que tout transfert vers des parties privées ou vers des autorités autres que des autorités répressives doit être strictement limité.

À la suite de négociations épineuses et de nombreux compromis politiques, la commission LIBE du Parlement européen a voté en faveur de son rapport le 21 octobre. Le rapport a été approuvé par le Parlement européen à sa première lecture lors d'un vote en séance plénière le 12 mars 2014. Au Conseil, les progrès sont restés plus limités. Les négociations entre les États membres se poursuivent sur des volets importants du cadre législatif, tels que le mécanisme de guichet unique et l'idée d'adopter un paquet législatif composé d'un règlement et d'une directive, parmi d'autres questions sensibles d'un point de vue politique et complexes sur le plan juridique.

Au cours de l'année 2013, nous avons continué de conseiller le Parlement européen et le Conseil et nous avons participé aux discussions. Nous avons également contribué au lancement du processus de révision du règlement (CE) nº 45/2001, qui régit le traitement des données par les institutions européennes, en adressant à la Commission une lettre exprimant nos positions initiales.

Chapitre quatre
Principaux développements dans les pays de l'EEE

ISLANDE

A. Résumé des activités et actualités

Le changement le plus imminent de la législation islandaise sur la protection des données susceptible d'avoir l'impact le plus important sur le travail actuel de la DPA était un avant-projet de loi sur la recherche scientifique dans le secteur de la santé. Ce projet de loi prévoyait que seul le comité national d'éthique pourrait délivrer des autorisations d'accès aux données sur la santé à des fins de recherche scientifique et que le rôle de la DPA à cet égard prendrait fin. D'un autre côté, le comité national d'éthique devait adresser à la DPA un résumé des autorisations délivrées pour que la DPA puisse décider quels projets de recherche elle souhaitait inspecter de plus près. Le comité national d'éthique ne serait pas autorisé à délivrer une autorisation avant un délai de 10 jours après l'envoi dudit résumé à la DPA. Si la DPA avisait le comité d'éthique de nouveaux contrôles pour un projet de recherche spécifique, le comité ne serait pas autorisé à délivrer d'autorisation avant que la DPA ait atteint une conclusion. D'après le projet de loi, la DPA pouvait émettre des ordonnances relatives aux mesures de sécurité applicables à la gestion de données à caractère personnel. Enfin, si la DPA estimait que le traitement de données à caractère personnel à des fins de recherche scientifique était en contradiction avec la loi nº 77/2000 sur la protection de la vie privée concernant le traitement des données à caractère personnel, le comité d'éthique ne serait pas autorisé à délivrer une autorisation pour un certain projet de recherche.

Un autre changement de la législation islandaise sur la protection des données a été la modification de la loi nº 163/2007 sur Statistics Iceland, le centre officiel des statistiques islandaises. Ce projet de modification de la loi prévoyait de confier à Statistics Iceland une vaste base de données sur des prêts personnels à des fins statistiques et aussi pour créer des mesures à prendre au bénéfice des foyers endettés. La DPA s'est opposée à un traitement aussi vaste et a souligné que le projet de loi n'expliquait pas la nécessité d'interventions aussi importantes dans la vie privée des personnes pour atteindre l'objectif du projet de loi, à savoir de créer des mesures au bénéfice des foyers endettés. Le Parlement a tenu compte des observations de la DPA et apporté des changements aux conditions de protection des données collectées, de durée de conservation et de suppression, notamment.

Enfin, un changement a été apporté à la loi nº 805/2013 sur la sécurité sociale. Ce qui concernait le plus le domaine de travail de la DPA était une disposition qui élargissait les pouvoirs de la sécurité sociale islandaise en matière de contrôle et de collecte de données d'autres organismes gouvernementaux tels que les autorités fiscales, la direction du travail, le registre national, certains fonds de pension, des maisons de repos, des municipalités, le fonds islandais pour les prêts aux étudiants, ainsi que d'autres organismes et sociétés. Le projet de loi prévoyait que cette collecte serait réalisée sans le consentement des personnes, contrairement à ce qui se faisait auparavant. La DPA a établi que la disposition du projet de loi sur la collecte des données sans consentement était trop vaste et ouverte, dans la mesure où elle ne déterminait pas de manière exhaustive les parties devant fournir des informations ni les informations pouvant être collectées sur la base de la disposition, et où le droit de la personne assurée à l'auto-détermination serait réduit sans raison. Les observations de la DPA ont été prises en compte et la disposition sur la collecte de données sans consentement a été annulée.

Organisation	Autorité de protection des données
Président et/ou collège	Sigrún Jóhannesdóttir, commissaire, jusqu'en avril 2013, date à laquelle Hörður Helgi Helgason est devenu commissaire ; Björg Thorarensen, présidente du Conseil d'administration.
Budget	66 millions d'ISK (environ 415 800 EUR, selon le taux de change au 31 décembre 2013)

Personnel	Trois conseillers juridiques, un secrétaire
Activités générales	
Décisions, avis, recommandations	Environ 120
Notifications	485
Contrôles préalables	118
Demandes émanant de personnes concernées	510
Plaintes émanant de personnes concernées	90
Conseils sollicités par le Parlement ou le gouvernement	Environ 50
Autres renseignements relatifs aux activités générales	Au total, 1 638 nouveaux cas ont été enregistrés en 2013
Activités d'inspection	
Contrôles, enquêtes	0 (en raison de ressources très limitées suite aux compressions financières)
Activités de sanction	
Sanctions	À l'exception des amendes journalières imposées 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 2013.
DPD	
Chiffres relatifs aux DPD	S. o.

B. Informations sur la jurisprudence

En mai 2013, le conseil de la DPA islandaise a traité une demande d'autorisation de traitement de DeCode Genetics ((Íslensk erfðagreining en islandais), une société qui analyse et effectue des recherches sur le génome humain, et de l'hôpital national (Landspítali). D'après la demande, l'hôpital national souhaitait transmettre un grand nombre d'informations à DeCode Genetics sur l'ensemble des personnes ayant bénéficié des services de l'hôpital sur une période de cinq ans. DeCode Genetics souhaitait ensuite associer ces données aux informations déjà collectées (y compris des données sur le génotype) auprès de personnes ayant pris part à d'autres projets de recherche de la société, soit 95 085 personnes au total, sans leur consentement. Les données devaient en outre être liées à des estimations générées par Íslensk erfðagreining sur les génotypes de 280 000 personnes qui n'avaient pas participé aux projets de recherche de la société, sans non plus obtenir leur consentement. La DPA a considéré ce traitement si important qu'il ne pouvait que s'appuyer sur la base juridique du consentement des personnes

concernées ou sur une loi répondant à de strictes conditions constitutionnelles. Aucune de ces conditions préalables n'étant remplie, la DPA a refusé de délivrer une autorisation. La DPA a par ailleurs ordonné à DeCode Genetics de supprimer les estimations de génotypes des personnes n'ayant pas participé à ses projets de recherche.

En août 2013, le conseil de la DPA islandaise a rendu un verdict concernant une société appelée Já, fondée en 2005 pour gérer l'annuaire téléphonique national et d'autres systèmes et solutions d'information. Já avait décidé de publier sur son site web un système présentant les photographies des zones urbaines avec une vue à 360° très similaire à celles de Google Street View. La présentation du projet de Já prévoyait que le traitement ne permettrait pas l'identification de personnes. L'application « street view » de Já a pourtant publié des photos identifiables dans lesquelles des visages et des plaques d'immatriculation étaient clairement reconnaissables. La DPA a considéré ces photos comme étant contraires à la loi nº 77/2000 et jugé que Já devait rendre ses photos inidentifiables. Já a ultérieurement confirmé à la DPA avoir flouté l'ensemble de ses photos identifiables.

LIECHTENSTEIN

A. Résumé des activités et actualités

En 2012, le bureau de la protection des données (DSS) a défini les thèmes de la santé et du bien-être social, du Liechtenstein en tant que centre financier, et de la sécurité des données comme les priorités des années à venir. Ces domaines sont des plus complexes. Des évolutions vont devoir être prévues aux niveaux international et européen pour assurer la protection de la sphère privée. Le rôle est et reste globalement dynamique et stimulant. Les premières mesures de la mise en œuvre de ces priorités ont été prises en 2013. La nécessité de définir ces priorités découle de l'étendue des sujets abordés d'une part, et des ressources limitées du bureau de la protection des données de l'autre.

L'éducation demeure la tâche la plus importante pour le DSS. Ces conclusions reposent, en particulier, sur une enquête représentative du DSS qui a montré que la population ignore encore beaucoup de choses sur la protection des données. Suite au scandale de la NSA, le DSS a rédigé et publié des conseils spécifiques sur la manière dont les personnes peuvent se protéger. Outre la traditionnelle journée de la protection des données, une table ronde sur le scandale de la NSA et son impact possible sur le Liechtenstein a été organisée avec l'association Verein Sicheres Liechtenstein. Le DSS a également organisé divers cours de formation, en mettant l'accent sur la sécurité des données et la communication sécurisée d'une part, et sur l'éducation des jeunes et des étudiants à l'utilisation des nouveaux médias de l'autre.

La disponibilité des ressources a également été élargie en faveur de la population et de groupes cibles particuliers, avec une ligne directrice sur le traitement des données à caractère personnel au travail, par exemple. Cette ligne directrice traite de la situation juridique et couvre tout, des candidatures aux références d'emplois. Elle envisage différents cas pratiques individuels, tels que l'utilisation des réseaux sociaux ou la pratique qui consiste à apporter ses appareils personnels sur le lieu de travail. Un modèle de déclaration de protection des données a également été créé pour les opérateurs de sites Internet, par exemple, ainsi qu'une recommandation portant sur les inscriptions. Ces outils sont disponibles sur le site web du DSS.[7]

Organisation	Bureau de la protection des données
Président et/ou collège	Philipp Mittelberger
Budget	596 000 EUR
Personnel	2,3 ETP aux affaires juridiques, 1,0 ETP à la technologie, 0,8 ETP à l'administration
Activités générales	
Décisions, avis, recommandations	10 autorisations relatives à des systèmes de vidéosurveillance
Notifications	À la fin de l'année, 308 ensembles de données au total avaient été inscrits au registre (un chiffre en baisse par rapport à l'année précédente, principalement en raison de la désignation de délégués à la protection des données par les autorités et les organisations privées, qui ont dès lors été exemptées de l'obligation de notification).

[7] http://www.llv.li/#/1758/datenschutzstelle

Contrôles préalables	S. o.
Demandes émanant de personnes concernées	98 demandes émanant de particuliers
Plaintes émanant de personnes concernées	S. o.
Conseils sollicités par le Parlement ou le gouvernement	10 réponses à des projets de loi
Other relevant general activity information	669 demandes (y compris de particuliers, voir ci-dessus)
Activités d'inspection	
Contrôles, enquêtes	6 contrôles réalisés
Activités de sanction	
Sanctions	S. o.
Amendes	S. o.
DPD	111 délégués à la protection des données
Chiffres relatifs aux DPD	

B. Informations sur la jurisprudence

Aucune décision de la Commission de protection des données n'a été publiée en 2013.

NORVÈGE

A. Résumé des activités et actualités

Une approche stratégique du conseil

Stratégiquement, il est important pour la DPA de participer activement dès le début à tout processus, et nous sommes heureux que les agences publiques, les organisations et les entreprises nous considèrent comme un interlocuteur important.

Respect de la vie privée dès la conception.

Ces dernières années, nous avons essayé de promouvoir les principes de respect de la vie privée dès la conception. Ceux-ci peuvent inclure la suppression automatique de données ou des solutions d'audit automatisées. Dans le livre blanc présenté au parlement norvégien (Storting), intitulé « Respect de la vie privée – perspectives et défis », il est établi que les principes de respect de la vie privée dès la conception doivent être utilisés lors du développement des solutions informatiques du gouvernement. Nous sommes heureux de cette évolution et avons l'intention de poursuivre ce travail à l'avenir.

L'année Snowden

2013 a été l'année où nous avons entendu parler d'Edward Snowden. La DPA a participé activement au débat qui a fait suite à ses révélations. Les limites de la surveillance exercée par un État vis-à-vis de ses citoyens sont des plus ténues. Le potentiel des technologies est illimité et, de notre point de vue, il était important d'affirmer qu'une surveillance de ce type n'était pas acceptable.

Technologies de services sociaux

Les technologies de services sociaux ont été l'un des points focaux de la DPA en 2013 et devraient le rester à l'avenir. Une nouvelle législation permet d'utiliser des technologies de suivi pour les personnes souffrant de démence, et l'accent est désormais mis sur les technologies de services sociaux elles-mêmes et la manière optimale dont elles peuvent être utilisées, plutôt que sur le droit d'utiliser ces technologies. Une fois encore, les principes de respect de la vie privée dès la conception pourraient bien porter leurs fruits.

En attendant, les technologies de services sociaux remettent en cause le respect de la vie privée. Nombre des solutions qui voient le jour aujourd'hui comprennent une part de surveillance. C'est la raison pour laquelle nous insistons sur l'équilibre entre l'utilité de la technologie et les conséquences sur la vie privée. En cas d'utilisation pour réduire autant que possible les conséquences grâce au consentement, à l'information et à une sécurité adéquate, etc., il est possible d'atteindre cet équilibre.

Publication du rapport « Mégadonnées – menaces sur les principes de respect de la vie privée »

La DPA a rédigé un rapport exhaustif qui souligne les défis pour la vie privée que soulève l'utilisation des mégadonnées. Le rapport propose également des conseils sur la manière d'utiliser les mégadonnées tout en respectant la vie privée des personnes. Nous y relevons les défis suivants :

- L'utilisation des données à de nouvelles fins
- La maximisation des données
- L'absence de transparence
- L'assemblage risque de constituer des informations sensibles

- Doit-on dire au revoir à l'anonymat ?
- Données – déterminisme
- Effet dissuasif

Suite à l'initiative de la DPA, le groupe de Berlin a décidé de créer un document de travail sur les mégadonnées. Le projet a été présenté aux membres du groupe de Berlin en septembre 2013, qui l'ont bien accueilli et devraient l'approuver lors de la prochaine réunion du groupe en mai 2014.

Organisation	Autorité norvégienne de protection des données
Président et/ou collège	Directeur Bjørn Erik Thon
Budget	37 millions de NOK
Personnel	41
Activités générales	
Décisions, avis, recommandations	S. o.
Notifications	8 912 nouvelles notifications enregistrées, 15 979 actives au total.
Contrôles préalables	155
Demandes émanant de personnes concernées	Au total, la DPA norvégienne a reçu 5 032 appels téléphoniques et 2 546 courriels adressés à nos services de conseils.
Plaintes émanant de personnes concernées	S. o.
Conseils sollicités par le Parlement ou le gouvernement	Nous avons reçu 134 invitations à commenter la nouvelle législation et envoyé des commentaires à 52 occasions.
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	Lieu de travail – 15 Secteur de la santé – 28 Justice et police – 5 Secteur public – 15 Établissements scolaires et éducation – 10 Autres – 3 **Total – 76**
Activités de sanction	
Sanctions	7 frais de pénalité, aucune amende coercitive, tous imposés par la

	DPA
Amendes	Total des amendes : 1 925 000 NOK.
DPD	
Chiffres relatifs aux DPD	210 DPD représentant 420 sociétés et bureaux publics au total.

B. Informations sur la jurisprudence

Gjensidige Insurance – Activités d'évaluation illégales

En mai 2013, la DPA a procédé à l'audit de Gjensidige Insurance. L'objet en était de contrôler son mode de traitement des données à caractère personnel et, notamment, dans le cadre d'enquêtes destinées à détecter des fraudes ou tentatives de fraude. L'audit a révélé l'existence de méthodes des plus intrusives dans le cadre de ces enquêtes. Ces méthodes faisaient en effet appel à l'observation dissimulée et à la surveillance audio et vidéo cachée pour prouver l'état de santé d'une personne. L'audit a également révélé d'importantes lacunes au niveau des procédures internes de la société en matière de gestion des informations personnelles en général. Nous avons jugé les déficiences si sérieuses que le risque de voir la société violer d'autres dispositions de la loi sur les données à caractère personnel était selon nous intolérable. Nous avons ordonné à la société de payer une amende de 600 000 couronnes, soit l'amende la plus élevée que la DPA ait imposée à ce jour. La société a également dû établir des procédures internes conformes à la loi sur les données à caractère personnel.

C. Autres informations importantes

Proposition de nouvelle loi sur les registres de santé (à des fins de traitement médical) et les revues médicales (à des fins secondaires).

En 2013, le ministère de la santé et des services de soins a proposé une nouvelle loi sur les dossiers médicaux et une nouvelle loi sur les revues médicales. La DPA soutient la proposition de diviser le règlement en deux lois différentes, une pour les dossiers médicaux portant sur des traitements, et une pour les dossiers médicaux à des fins de gestion, d'administration et de recherche.

D'un autre côté, nous avons trouvé la proposition très préoccupante, notamment, en ce qui concerne l'affaiblissement du droit d'un patient à l'autodétermination.

Chapitre cinq

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

MEMBRES DU GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES EN 2013

Allemagne	Autriche
M. Peter Schaar Commissaire fédéral à la protection des données et à la liberté de 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 de Berlin pour la protection des données et la liberté de l'information (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 Commission autrichienne de la protection des données (Datenschutzkommission) Hohenstaufengasse 3 - AT - 1014 Vienne Tél. : +43 1 531 15 / 202525 Fax : +43 1 531 15 / 202690 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 (Commissie voor de bescherming van de persoonlijke levenssfeer) Rue de la Presse, 35 - 1000 Bruxelles Tél. : +32 2 274 48 00 Fax : +32 2 274 48 35 Adresse électronique : commission@privacycommission.be	M. Ventsislav Karadjov Commission de protection des données à caractère personnel – CPDP (Комисия за защита на личните данни) 2 Prof. Tsvetan Lazarov Blvd. Sofia 1592 Tél. : + 359 2 915 35 31 Fax : + 359 2 915 35 25 Adresse électronique : kzld@cpdp.bg

Site web : http://www.privacycommission.be/	Site web : http://www.cdpd.bg
Chypre	**Danemark**
M. Yiannos Danielides Commissaire à la protection des données à caractère personnel (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2e - CY - 1082 Nicosie (P.O. Box 23378 - CY - 1682 Nicosie) Tél. : +357 22 818 456 Fax : +357 22 304 565 Adresse électronique : commissioner@dataprotection.gov.cy Site web : http://www.dataprotection.gov.cy	(Temp.) Mme Birgit Kleis Agence danoise de protection des données (Datatilsynet) Borgergade 28, 5e - DK - 1300 Copenhague 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) 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	M. Viljar Peep Autorité de contrôle de la protection des données estonienne (Andmekaitse Inspektsioon) 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	**France**

M. Reijo Aarnio Bureau du médiateur chargé de la protection des données (Tietosuojavaltuutetun toimisto) Ratapihantie 9, 6e - FIN – 00521 Helsinki (P.O. Box 800) Tél. : +358 295 666 700 Fax : +358 295 666 735 Adresse électronique : tietosuoja@om.fi Site web : http://www.tietosuoja.fi	Mme Isabelle Falque Pierrotin Présidente Présidente de l'autorité française de protection des données (Commission nationale de l'informatique et des libertés – CNIL) Rue Vivienne, 8 - CS 30223 FR - 75083 Paris Cedex 02 Tél. : +33 1 53 73 22 22 Fax : +33 1 53 73 22 00 Adresse électronique : Ifalquepierrotin@cnil.fr Site web : http://www.cnil.fr
Grèce	**Hongrie**
M. Petros Christoforos Autorité hellénique de protection des données (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Athènes Tél. : +30 210 6475608 Fax : +30 210 6475789 Adresse électronique : p.christoforos@DPA.gr Site web : http://www.DPA.gr	M. Attila Péterfalvi Président de l'autorité nationale pour la protection des données et la liberté de l'information Szilágyi Erzsébet fasor 22/C H-1125 Budapest Tél. : +36 1 3911 400 Adresse électronique : ugyfelszolgalat@naih.hu Site web : http://www.naih.hu
Irlande	**Italie**
M. Billy Hawkes Commissaire à la protection des données (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE - Co. Laois Tél. : +353 57 868 4800 Fax :+353 57 868 4757 Adresse électronique : info@dataprotection.ie Site web : http://www.dataprotection.ie	M. Antonello Soro Autorité italienne de protection des données (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Rome Tél. : +39 06.69677.1 Fax : +39 06.69677.785 Adresse électronique : garante@garanteprivacy.it, a.soro@garanteprivacy.it Site web : http://www.garanteprivacy.it
Lettonie	**Lituanie**
Mme Signe Plumina	M. Algirdas Kunčinas

Inspection nationale des données de Lettonie (Datu valsts inspekcija) Blaumaņa iela 11/13-15 Riga, LV-1011 Tél. : + 371 67223131 Adresse électronique : info@dvi.gov.lv Site web : www.dvi.gov.lv	Inspection nationale de protection des données (Valstybinė duomenų apsaugos inspekcija) A.Juozapaviciaus str. 6 / Slucko str. 2, LT-01102 Vilnius Tél. : +370 5 279 14 45 Fax : + 370 5 261 94 94 Adresse électronique : ada@ada.lt Site web : http://www.ada.lt
Luxembourg	**Malte**
M. Gérard Lommel Commission nationale pour la protection des données (CNPD) 1, avenue du Rock'n'Roll L - 4361 Esch-sur-Alzette Tél. : +352 26 10 60 - 1 Fax : +352 26 10 60 - 29 Adresse électronique : info@cnpd.lu Site web : http://www.cnpd.lu	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 High Street Sliema SLM 1549 Tél. : +356 2328 7100 Fax : +356 23287198 Adresse électronique : joseph.ebejer@gov.mt Site web : http://www.idpc.gov.mt
Pays-Bas	**Pologne**
M. Jacob Kohnstamm Autorité néerlandaise de protection des données (College Bescherming Persoonsgegevens – CBP) Juliana van Stolberglaan 4-10, P.O. Box 93374 2509 AJ La Haye Tél. : +31 70 8888500 Fax : +31 70 8888501 Adresse électronique : info@cbpweb.nl/international@cbpweb.nl Site web : www.cbpweb.nl/www.mijnprivacy.nl	M. Wojciech Rafał Wiewiórowski Inspecteur général pour la protection des données à caractère personnel (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Varsovie Tél. : +48 22 860 73 12 ; +48 22 860 70 81 Fax : +48 22 860 73 13 Adresse électronique : desiwm@giodo.gov.pl Site web : http://www.giodo.gov.pl
Portugal	**République tchèque**
Mme Filipa Calvão Commission nationale de protection des données	M. Igor Nemec Bureau de la protection des données à caractère

(Comissão Nacional de Protecção de Dados – CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lisbonne Tél. : +351 21 392 84 00 Fax : +351 21 397 68 32 Adresse électronique : geral@cnpd.pt Site web : http://www.cnpd.pt	personnel (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 - CZ - 170 00 Prague 7 Tél. : +420 234 665 111 Fax : +420 234 665 501 Adresse électronique : posta@uoou.cz Site web : http://www.uoou.cz/
Roumanie	**Royaume-Uni**
Mme Ancuța Gianina Opre Autorité nationale de contrôle du traitement des données à caractère personnel (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Gen. Gheorghe Magheru Bld. 28-30, 1st District, RO - Bucarest Tél. : +40 31 805 9211 Fax : +40 31 805 9602 Adresse électronique : anca.opre@dataprotection.ro international@dataprotection.ro Site web : www.dataprotection.ro	M. Christopher Graham Bureau du commissaire à l'information Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tél. : 0303 123 1113 (tarif local) Tél. : +44 1625 545745 (tarif national) Fax : +44 1625 524510 Adresse électronique : veuillez compléter le formulaire de demande sur notre site web Site web : http://www.ico.org.uk
Slovaquie	**Slovénie**
Mme Eleonóra Kročianová Bureau de protection des données à caractère personnel de la République slovaque (Úrad na ochranu osobných údajov Slovenskej republiky) Hraničná 12 - SK - 82007 Bratislava 27 Tél. : +421 2 3231 3211 Fax : +421 2 3231 3234 Adresse électronique : statny.dozor@pdp.gov.sk Site web : http://www.dataprotection.gov.sk	Mme Natasa Pirc Musar Commissaire à l'information (Informacijski pooblaščenec) Vošnjakova 1, SI - 1000 Ljubljana Tél. : +386 1 230 97 30 Fax : +386 1 230 97 78 Adresse électronique : gp.ip@ip-rs.si Site web : http://www.ip-rs.si
Suède	**Contrôleur européen de la protection des données**
Mme Kristina Svahn Starrsjö Conseil de l'inspection des données	M. Peter Hustinx Contrôleur européen de la protection des données – CEPD

(Datainspektionen) Drottninggatan 29, 5e Box 8114 - SE - 104 20 Stockholm Tél. : +46 8 657 61 57 Fax : +46 8 652 86 52 Adresse électronique : datainspektionen@datainspektionen.se Site web : http://www.datainspektionen.se	Adresse postale : 60, rue Wiertz, BE - 1047 Bruxelles Bureau : 30, rue Montoyer, BE - 1000 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 « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES EN 2013

Ancienne République yougoslave de Macédoine	Islande
M. Dimitar Gjeorgjievski Direction pour la protection des données à caractère personnel (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tél. : +389 2 3230 635 Fax : +389 2 3230 635 Adresse électronique : info@dzlp.mk Site web : www.dzlp.mk	M. Hörður Helgi Helgason Directeur 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 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 juridique Autorité norvégienne de protection 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	
Mme Dubravka Dolenc Directrice adjointe Mme Sanja Silaj Zeman Chef du département de la coopération internationale et des affaires juridiques et européennes Agence croate de protection des données à caractère personnel (Agencija za zaštitu osobnih podataka – AZOP) Martićeva 14, 10000 Zagreb Tél. : +385 1 4609-000	

Fax : +385 1 4609 099 Adresse électronique : azop@azop.hr ou sanja.silaj-zeman@azop.hr Site web : http://www.azop.hr	

Secrétariat du groupe de travail « Article 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-15-002-FR-N

Office des publications

ISBN 978-92-79-52065-5
doi:10.2838/17385