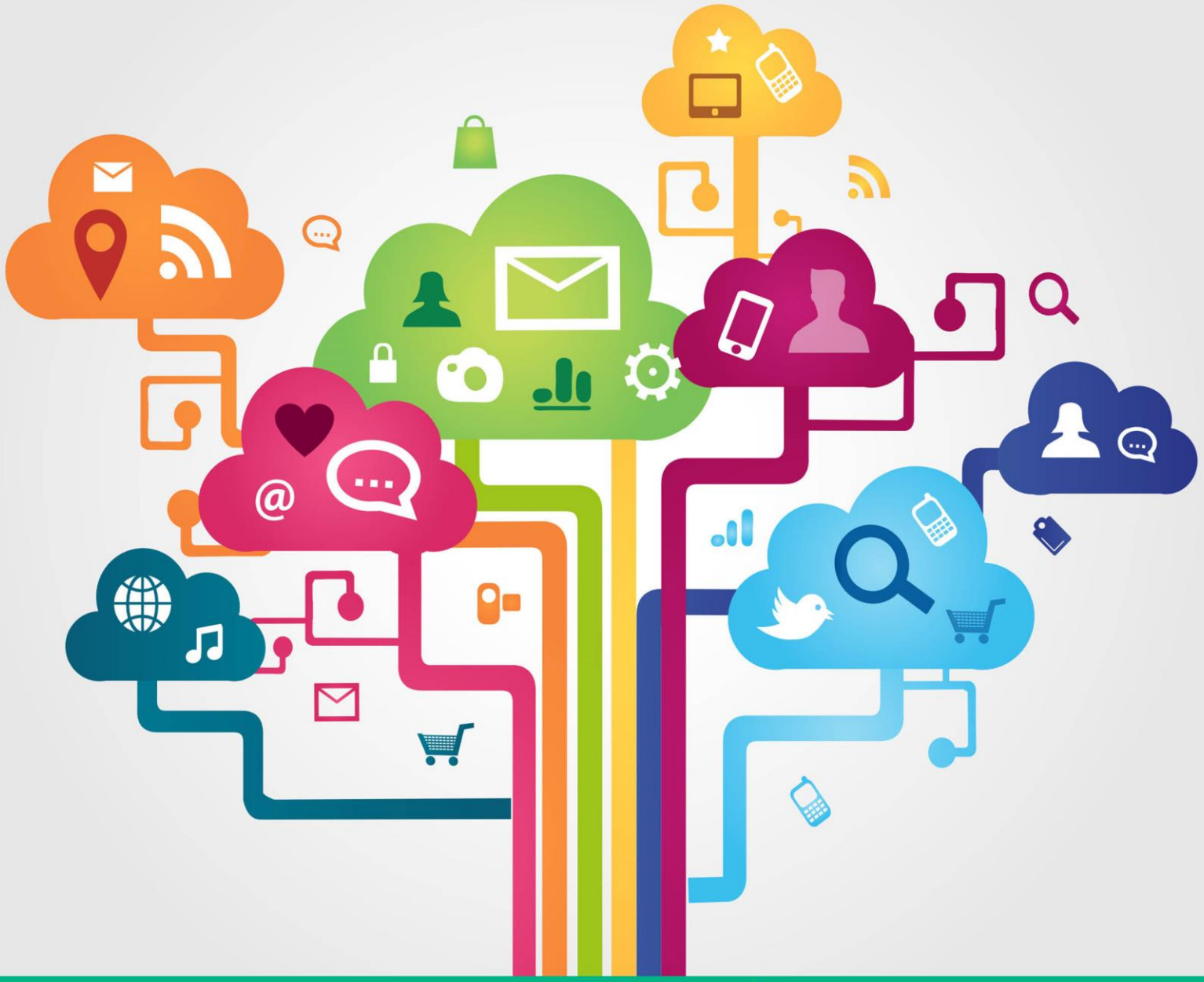
Commission européenne



Seizième rapport

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

Portant sur l'année 2012

Adopté le 25 novembre 2014

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).

Luxembourg: Office des publications de l'Union européenne, 2015

PDF	978-92-79-44094-6	2363-1007	10.2838/202799	DS-AA-15-001-FR-N

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

Portant sur l'année 2012

Table des matières

AVANT-PROPOS DU PRÉSIDENT DU GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES 0

QUESTIONS EXAMINÉES PAR LE GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES 1

1.1. Transfert de données vers des pays tiers 2

1.1.1 Adéquation 2

1.1.2 Règles d'entreprise contraignantes (BCR) 3

1.2 Communications électroniques, Internet et nouvelles technologies 4

1.3 Révision du cadre juridique de la protection des données 8

1.4. Données à caractère personnel 11

1.4.1 epSOS 11

1.4.2 Évolution des technologies biométriques 12

PRINCIPAUX DÉVELOPPEMENTS AU SEIN DES ÉTATS MEMBRES 14

Allemagne 15

Autriche 19

Belgique 23

Bulgarie 27

Chypre 34

Danemark 37

Espagne 40

Estonie 44

Finlande 50

France 54

Grèce 59

Hongrie 64

Irlande 70

Italie 73

Lettonie 79

Lituanie 83

Luxembourg 86

Malte 89

Pays-Bas 92

Pologne 95

Portugal 101

_____République Tchèque 103

_____Roumanie 107

_____Royaume-Uni 111

_____Slovaquie 117

_____Slovénie 123

_____Suède 129

UNION EUROPÉENNE ET ACTIVITÉS COMMUNAUTAIRES 131

_____3.1. Commission européenne 132

_____3.2. Cour de justice de l'union européenne 137

_____3.3. Contrôleur européen de la protection des données 140

PRINCIPAUX DÉVELOPPEMENTS DANS LES PAYS DE L'EEE 144

_____Islande 145

_____Liechtenstein 148

_____Norvège 150

MEMBRES ET OBSERVATEURS DU GROUPE DE TRAVAIL « ARTICLE 29 »
SUR LA PROTECTION DES DONNÉES 153

_____Membres du groupe de travail « article 29 » sur la protection des données en 2012 154

_____Observateurs du groupe de travail « article 29 » sur la protection des données en 2012 160

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

L'année 2012 promettait d'être très importante pour la protection des données dans l'Union européenne et très intéressante pour le groupe de travail « Article 29 ». En 2012, la Commission européenne devait présenter ses propositions de nouveau cadre juridique sur la protection des données au sein de l'UE. Étant donné qu'en 2009, le groupe de travail avait déjà commencé à fournir à la Commission des informations pour ce nouveau cadre juridique, la présentation des propositions devait être un moment très importarent.

Et en janvier 2012, la Commission européenne a effectivement présenté sa proposition de nouveau cadre juridique sur la protection des données au sein de l'UE, consistant en un règlement général sur la protection des données et en une directive applicable dans le domaine de la police et de la justice.

La proposition a globalement reçu un excellent accueil de la part du groupe de travail. Le fait que l'instrument choisi ait été un règlement directement applicable à tous les États membres de l'UE représente un grand pas en avant. Bien que la proposition consiste en deux instruments différents, la législature peut toujours en assurer l'exhaustivité dès lors qu'elle traite le règlement et la directive comme un ensemble reposant sur des droits et principes de base identiques.

Naturellement, des doutes subsistent. Par exemple, le groupe de travail estime que le principe de limitation de la finalité, qui est l'un des principes de base de la protection des données, pourrait être sérieusement mis à mal par l'introduction de la disposition selon laquelle, si un nouveau fondement juridique pouvait être trouvé, les données pourraient servir à des finalités différentes, voire incompatibles. Naturellement, il est parfois nécessaire de pouvoir utiliser des données à d'autres fins, mais celles-ci doivent néanmoins rester compatibles avec les finalités pour lesquelles les données ont initialement été collectées. Se contenter de rechercher un fondement juridique différent ne saurait suffire.

Nonobstant le rôle de gardienne des traités dévolu à la Commission, de fortes réserves ont été formulées quant au rôle prévu pour la Commission, dans le sens où de nombreuses dispositions pourraient empiéter sur l'indépendance des DPA. Lorsqu'une question est examinée ou a été examinée par le CEPD dans le cadre du mécanisme de contrôle de la cohérence, la Commission devrait être en mesure de donner son appréciation juridique tout en s'abstenant en principe d'intervenir.

Par ailleurs, il peut naturellement être nécessaire de laisser certaines questions à des actes délégués et/ou d'exécution. Toutefois, toutes les questions pour lesquelles sont prévus des actes délégués ou d'exécution ne peuvent pas être adéquatement traitées par le biais de ces instruments. Dans certains cas, la question concernée ne constitue pas un point de détail et devrait être reprise dans le texte du règlement lui-même, tandis que dans d'autres cas, des lignes directrices du comité européen de la protection des données (CEPD) seraient un instrument plus approprié.

Après la présentation de la proposition, le Parlement européen (PE) et le Conseil ont initié leurs procédures législatives respectives. Au moment de la rédaction de ce rapport, le comité responsable du Parlement européen (LIBE) avait fini ses discussions et adopté sa position sur la base de laquelle le PE entamera les négociations. Au sein du Conseil, toutefois, les discussions sont toujours en cours.

Les développements techniques et la mondialisation croissante de notre société rendent de plus en plus nécessaires l'adaptation à l'avenir et l'actualisation du cadre juridique de la protection des données au sein de l'UE.

C'est la raison pour laquelle il est permis d'espérer que les discussions du Conseil donnent prochainement lieu à une position commune des États membres permettant aux négociations (ou trilogue) de commencer rapidement en vue de l'adoption d'un nouveau cadre juridique à l'été 2014.

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 Adéquation

Avis 7/2012 (WP198) sur le niveau de protection des données à caractère personnel dans la Principauté de Monaco

En 2009, la Principauté de Monaco a demandé à la Commission d'évaluer si elle assurait un niveau adéquat de protection des données personnelles au sens de l'Article 25(6) de la directive 95/46/CE, et de prendre une décision à cet égard. Dans le cadre de la procédure d'évaluation du caractère adéquat de ce niveau de protection, la Commission a demandé l'avis du groupe de travail « Article 29 ».

En raison des liens historiques qui unissent la France et Monaco, la législation monégasque relative à la protection des données est proche de la législation française en la matière. L'Article 20 de la Constitution de Monaco confirme la protection du droit à la vie privée et dispose que **«** Toute personne a droit au respect de sa vie privée et familiale et au secret de sa correspondance **»**.

La protection des données à caractère personnel est régie par la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives (modifiée par la loi n° 1.353 du 4 décembre 2008 et par la loi n° 1.353 du 1er avril 2009), et par l'Ordonnance Souveraine n° 2.230 du 29 juin 2009 fixant les modalités d'application de la loi.

L'évaluation du groupe de travail porte essentiellement sur la loi n° 1.165 telle que modifiée en 2008 et 2009, et fait référence aux principales dispositions de la directive, en tenant compte des lignes directrices énoncées dans son document de travail, « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données », adopté le 24 juillet 1998 (WP 12).

Cette loi institue l'autorité de protection des données de Monaco, la Commission de Contrôle des Informations Nominatives (CCIN), en tant qu'autorité indépendante. La CCIN a publié différents guides, délibérations et rapports d'activité annuels, ainsi que d'autres informations sur divers sujets tels que la biométrie, les puces GPS, la vidéosurveillance, etc. afin de définir les droits et obligations des personnes physiques, des entreprises et de l'État, et de fournir des orientations sur l'application pratique des principes relatifs au respect de la vie privée.

À l'échelle internationale, Monaco a signé et ratifié en 2005 la Convention européenne des droits de l'homme, la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) et son Protocole additionnel (en vigueur depuis le 1er avril 2009), ainsi que le Pacte international relatif aux droits civils et politiques, le 28 août 1997.

Le groupe de travail a considéré que le champ d'application de la loi monégasque sur la protection des données était semblable à celui de la directive, même si certaines modifications apportées au libellé actuel préciseraient mieux, semble-t-il, les modalités d'application des dispositions de cette loi aux personnes morales.

Le groupe de travail a estimé que la législation était conforme aux principes de qualité et de proportionnalité des données, au principe de transparence et au principe de sécurité, ainsi qu'aux droits d'accès, de rectification et d'opposition, à condition que les exceptions fassent l'objet d'une interprétation stricte.

La législation monégasque a été considérée comme conforme au principe de transfert ultérieur et, de manière générale, aux exigences relatives aux catégories particulières de données.

Même si les dispositions relatives au droit d'opposition en cas de marketing direct auraient pu être plus claires, des garanties acceptables ont été mises en place à cet égard. La législation a également été considérée comme conforme au « principe de décisions individuelles automatisées ».

Le groupe de travail a estimé que l'objectif consistant à assurer un niveau satisfaisant de respect des règles n'était que partiellement atteint, et a suggéré l'adoption de dispositions visant une mise en œuvre plus efficace de l'indépendance structurelle et financière de la CCIN, ainsi que le renforcement des pouvoirs coercitifs conférés à la CCIN quant au respect par le secteur public et, plus généralement, quant aux mesures à imposer aux responsables de traitement qui ne respectent pas la loi, indépendamment et au-delà de l'imposition de sanctions pénales par les autorités judiciaires.

Le groupe de travail a estimé que la législation de Monaco établissait des mécanismes suffisants pour apporter aide et assistance aux personnes physiques, et garantissait suffisamment le droit de la personne concernée d'être indemnisée pour tout dommage portant atteinte à ses droits ou à ses biens et consécutif au traitement illicite de données à caractère personnel.

Le groupe de travail a conclu que la Principauté de Monaco garantissait un niveau adéquat de protection des données personnelles au sens de l'Article 25 (6) de la directive 95/46/CE, tout en suggérant d'y inclure des notions telles que celles de « fichier », « tiers », « sous-traitant », « consentement de la personne concernée » ; de clarifier les modalités d'application des dispositions de la loi aux personnes morales ; de clarifier le droit des personnes concernées d'être informées en temps utile (notamment lorsque les données n'ont pas été obtenues directement auprès de la personne concernée), et de s'opposer sans motifs légitimes au traitement à des fins de marketing direct. Les pouvoirs coercitifs dévolus à l'autorité devraient également être renforcés en ce qui concerne le respect des dispositions légales par le secteur public et les mesures à imposer aux responsables de traitement qui ne respectent pas la loi.

1.1.2 Règles d'entreprise contraignantes (BCR)

Document de travail 02/2012 (WP 195) établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants

Afin de faciliter l'application des règles d'entreprise contraignantes (ci-après les « BCR ») pour les responsables du traitement dans le document « BCR pour vos données personnelles » (WP 153), le groupe de travail « Article 29 » a déjà mis au point des outils visant à régir les transferts de données à caractère personnel qui sont traitées, à l'origine, par l'entreprise agissant en tant que responsable du traitement (telles que les données relatives aux clients de l'entreprise, à ses salariés, etc.).

Ce document a pour objet de proposer une boîte à outils décrivant les conditions à respecter, de manière à rendre l'utilisation des BCR plus aisée pour les sous-traitants (« BCR concernant les données relatives à des tiers »).

Les BCR pour les sous-traitants visent à régir les transferts internationaux de données à caractère personnel qui sont initialement traitées par l'entreprise en tant que sous-traitant de données, conformément aux instructions externes d'un responsable du traitement des données (notamment pour les activités de sous-traitance). Conformément à la directive 95/46/CE, un contrat doit être conclu entre le responsable du traitement et le sous-traitant. Ce contrat est désigné ci-après par l'expression « contrat de service ».

Recommandation 7/2012 (WP 195a) sur le formulaire de demande standard pour l'approbation des règles d'entreprise contraignantes pour le transfert de données à caractère personnel dans le cadre d'activités de traitement

En conjonction avec la boîte à outils développée pour les règles d'entreprise contraignantes pour les sous-traitants, avec la présente recommandation, le groupe de travail a adopté un formulaire de demande standard pour l'approbation du traitement conformément à ces règles d'entreprise contraignantes.

1.2 COMMUNICATIONS ÉLECTRONIQUES, INTERNET ET NOUVELLES TECHNOLOGIES

Avis 06/2012 (WP 197) sur le projet de décision de la Commission concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE sur la vie privée et les communications électroniques

Cet avis porte sur les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE sur la vie privée et les communications électroniques qui, pour des raisons techniques, était initialement un projet de décision de la Commission avant de devenir un règlement.

Dans son avis, le groupe de travail se félicite des efforts de précision de la Commission pour clarifier les dispositions de la directive 2002/58/CE concernant la violation de données à caractère personnel, mais laisse entendre que certains des termes utilisés auraient pu être exprimés plus précisément.

Concernant la notification à l'autorité compétente, le groupe de travail se félicite du fait que des délais précis figurent dans le règlement et soutient la procédure de notification en deux temps, qui permet de combiner réactivité et exhaustivité.

Concernant les informations à transmettre et la notification initiale, le groupe de travail estime que, pour encourager les fournisseurs à mettre en œuvre une politique de sécurité des données à caractère personnel de qualité, le fournisseur devrait être invité à fournir toutes les informations dont il dispose au cours de la première phase de notification, y compris le type de données à caractère personnel concerné, les circonstances de la violation ou du type d'exposition (perte, vol, reproduction, etc.) et la manière dont la violation a été constatée (logiciel de détection installé, analyse des registres, un employé a signalé un incident, etc.).

Concernant le moyen électronique, le groupe de travail soutient l'initiative de la Commission européenne visant à promouvoir un tel moyen quand cela est possible, mais avertit que la mise en œuvre de ce moyen électronique dans tous les États membres n'est pas immédiate : il sera nécessaire de définir un format de notification électronique commun, d'adopter des mesures de sécurité adéquates, de développer et de tester le moyen électronique (portail et/ou autre système tel qu'une messagerie sécurisée) qui étayera ce mécanisme dans chaque État membre.

Concernant la notification aux autres autorités nationales concernées, le groupe de travail accueille favorablement et soutient une coopération active entre les autorités, et il comprend clairement la nécessité d'une coopération entre les autorités nationales compétentes. Il recommande toutefois à la Commission de préciser le champ d'application de la disposition correspondante et de clarifier les moyens pratiques que les autorités compétentes devraient utiliser pour coopérer.

Concernant la notification à l'abonné ou au particulier, le groupe de travail se félicite du fait que le règlement décrit une procédure dans les cas où les personnes ne peuvent être directement contactées. Le groupe de travail salue également la description des circonstances à prendre en considération pour déterminer si une violation de données à caractère personnel porte atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une personne.

Concernant l'évaluation de la gravité et des effets négatifs, le groupe de travail a établi la nécessité d'une méthode d'évaluation uniforme et facile à comprendre tant pour les fournisseurs que pour les autorités compétentes en Europe. La décision bénéficierait grandement d'orientations plus détaillées à cet égard. Pour répondre à ces exigences, le groupe de travail soutient résolument la mise en œuvre d'une méthode d'évaluation de la gravité qui soit harmonisée, paneuropéenne et fondée sur des critères objectifs.

Concernant les mesures de protection technologiques et l'incompréhensibilité des données, le groupe de travail se félicite de telles mesures et estime qu'elles conduiront les parties intéressées vers de meilleures pratiques de sécurité, tout en assurant une sécurité juridique plus forte quant à la notion de données incompréhensibles dans tous les États membres. Toutefois, ce règlement ne doit pas donner aux opérateurs l'impression que le fait de recourir au cryptage, au hachage ou à la suppression sécurisée est suffisant en soi pour que les fournisseurs puissent prétendre avoir rempli l'obligation générale de sécurité

énoncée à l'article 17 de la directive 95/46/CE — les fournisseurs devraient également mettre en œuvre les mesures techniques et d'organisation appropriées pour prévenir, détecter et empêcher les violations de données à caractère personnel.

Le groupe de travail fait par ailleurs observer que le projet de règlement ne comporte pas de disposition ou de considérant concernant l'inventaire mentionné à l'article 4, paragraphe 4, de la directive. Compte tenu des liens étroits existant entre les notifications et l'inventaire, le groupe de travail a proposé d'ajouter un considérant à la décision afin de souligner que les fournisseurs pourront aussi se reporter au règlement pour définir le format des entrées de l'inventaire. De même, le projet de règlement indique que les autorités établissent des statistiques concernant les violations. Le groupe de travail suggère que la décision inclue un ensemble harmonisé d'éléments à contrôler sur le plan statistique.

Avis 05/2012 (WP 196) sur l'informatique en nuage

Dans cet avis, le groupe de travail « Article 29 » analyse toutes les questions intéressant les fournisseurs de services d'informatique en nuage qui exercent leurs activités dans l'espace économique européen (EEE) ainsi que leurs clients, en précisant, lorsque c'est utile, tous les principes applicables tirés de la directive de l'UE relative à la protection des données (95/46/CE) et de la directive « vie privée et communications électroniques » 2002/58/CE (modifiée par la directive 2009/136/CE).

Tout en reconnaissant les avantages indéniables que l'informatique en nuage présente pour l'économie et la société, cet avis décrit comment son utilisation généralisée peut créer un certain nombre de risques pour la protection des données, tenant principalement à une absence de contrôle sur les données à caractère personnel et à une information insuffisante sur le mode et le lieu du traitement ou du sous-traitement des données et sur la ou les personnes qui les réalisent. Ces risques doivent être soigneusement évalués par les organismes publics et les entreprises privées qui envisagent de recourir aux services d'un fournisseur d'informatique en nuage.

Cet avis examine les questions liées au partage de ressources avec des tiers, au manque de transparence que comporte une chaîne d'externalisation composée de multiples sous-traitants, à l'absence de cadre commun mondial régissant la portabilité des données, et à l'incertitude qui entoure l'admissibilité du transfert des données à caractère personnel aux fournisseurs d'informatique en nuage établis en dehors de l'EEE. De la même façon, il souligne les graves préoccupations que suscite le manque de transparence des informations qu'un responsable du traitement doit être en mesure de présenter à une personne concernée sur la manière dont ses données à caractère personnel sont traitées. Les personnes concernées doivent savoir qui traite leurs données et à quelles fins, pour être en mesure d'exercer les droits qui leur sont conférés à cet égard.

L'une des principales conclusions tirées par cet avis est que les entreprises et les administrations qui souhaitent recourir à l'informatique en nuage devraient, dans un premier temps, procéder à une analyse de risques rigoureuse et exhaustive. Tous les fournisseurs d'informatique en nuage qui offrent des services dans l'EEE devraient communiquer à leurs clients toutes les informations qui leur sont nécessaires pour évaluer correctement les avantages et les inconvénients d'un tel service. La sécurité, la transparence et la sécurité juridique des clients devraient occuper une place essentielle dans l'offre de services d'informatique en nuage.

Le groupe de travail se félicite des dispositions figurant à l'article 26 de la proposition de règlement de la Commission qui tendent à rendre les sous-traitants plus responsables envers les responsables du traitement en les aidant à assurer le respect, notamment, de leurs obligations en matière de sécurité et de leurs obligations connexes. L'article 30 de la proposition prévoit l'obligation juridique pour le sous-traitant de mettre en œuvre les mesures techniques et organisationnelles qui s'imposent. Le projet de proposition précise qu'un sous-traitant qui ne se conforme pas aux instructions du responsable du traitement devient responsable du traitement et se trouve alors soumis aux règles spécifiques en matière de contrôle conjoint.

Le groupe de travail estime que cette proposition va dans la bonne direction pour remédier au déséquilibre qui caractérise généralement l'environnement d'informatique en nuage, dans lequel le client (particulièrement s'il est une PME) peut avoir du mal à exercer le plein contrôle exigé par la législation sur la protection des données sur la façon dont le fournisseur fournit les services demandés. De plus, les personnes concernées et les petites entreprises utilisatrices ne se trouvant pas dans la même situation juridique face aux grands fournisseurs d'informatique en nuage, il est recommandé aux clients et aux entreprises commerciales de jouer un rôle plus dynamique pour négocier des conditions générales plus équilibrées auprès de ces fournisseurs.

Le groupe de travail estime que, dans l'intérêt de la sécurité juridique des personnes concernées dont les données à caractère personnel sont stockées dans des centres de données à travers le monde, il est primordial que le futur règlement prévoie d'interdire aux responsables du traitement qui exercent leurs activités dans l'UE de communiquer des données à caractère personnel à un pays tiers sur la demande des autorités judiciaires ou administratives de ce pays, sauf autorisation expresse découlant d'un accord international ou approbation de l'autorité de contrôle.

Les organismes publics devraient évaluer en premier lieu si la communication, le traitement et le stockage des données en dehors du territoire national peuvent présenter des risques inacceptables de sécurité et de protection de la vie privée pour les citoyens et pour la sécurité nationale et l'économie – en particulier lorsque des bases de données sensibles (comme les données de recensement) ou des services stratégiques (comme les soins médicaux) sont en jeu. De ce point de vue, les gouvernements nationaux et les institutions de l'Union européenne pourraient envisager de poursuivre l'étude d'un nuage gouvernemental européen qui constituerait un espace virtuel supranational où pourraient s'appliquer des règles uniformes et harmonisées.

Le groupe de travail soutient la stratégie de partenariat européen dans le domaine du nuage informatique qui suppose la passation de marchés publics informatiques pour stimuler le marché européen des services en nuage. Le transfert de données à caractère personnel à un fournisseur européen d'informatique en nuage, tenu en dernier ressort de respecter la législation européenne sur la protection des données, pourrait apporter des avantages considérables aux consommateurs en matière de protection des données, notamment en favorisant l'adoption de normes communes (particulièrement dans le domaine de l'interopérabilité et de la portabilité des données) et la sécurité juridique.

Avis 04/2012 (WP 194) sur l'exemption de l'obligation de consentement pour certains cookies

L'article 5, paragraphe 3, de la directive 2002/58/CE telle que modifiée par la directive 2009/136/CE a renforcé la protection des utilisateurs de réseaux et services de communications électroniques en exigeant que le stockage d'informations ou l'obtention de l'accès à des informations dans l'équipement terminal d'un utilisateur (ou abonné) ne soit permis qu'à condition que ce dernier ait donné son consentement informé.

Cette exigence s'applique à tous les types d'informations stockées ou accessibles dans l'équipement terminal de l'utilisateur. Cet avis traite de l'incidence du nouvel article 5, paragraphe 3, sur l'utilisation des cookies, mais ce terme ne doit pas être considéré comme excluant les technologies similaires.

L'article 5, paragraphe 3, permet d'exempter certains cookies de l'obligation de consentement informé s'ils satisfont à l'un des critères suivants : le cookie vise « exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques », ou le cookie est « strictement nécessaire au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur ».

Dans la mesure où le groupe de travail a déjà examiné les exigences relatives au consentement informé de manière détaillée, ce document vise à analyser les exemptions à ce principe dans le contexte des cookies et des technologies apparentées.

L'analyse du groupe de travail suggère que les cookies suivants peuvent être exemptés de l'obligation de consentement informé à certaines conditions s'ils ne sont pas utilisés à d'autres fins : les cookies

alimentés par l'utilisateur, pour la durée d'une session, ou les cookies persistants limités à quelques heures dans certains cas ; les cookies d'authentification, utilisés pour des services authentifiés, pour la durée d'une session ; les cookies de sécurité centrés sur l'utilisateur, utilisés pour détecter les authentifications abusives, pour une durée limitée répétée ; les cookies de session créés par un lecteur multimédia, tels que les cookies de lecteur flash, pour la durée d'une session ; les cookies de session d'équilibrage de charge, pour la durée d'une session ; les cookies persistants de personnalisation de l'IU, pour la durée d'une session (ou une durée légèrement supérieure) ; les cookies de modules sociaux de tiers pour le partage de contenu, pour les membres connectés à un réseau social.

Pour ce qui est des réseaux sociaux, le groupe de travail note cependant que l'utilisation de cookies de modules sociaux de tiers à d'autres fins que la fourniture d'une fonctionnalité expressément demandée par leurs propres membres requiert un consentement, notamment si ces finalités impliquent de pister les utilisateurs d'un site web à l'autre.

Le groupe de travail rappelle que les cookies publicitaires de tiers ne peuvent être exemptés de l'obligation de consentement et précise en outre que le consentement est également nécessaire pour des finalités opérationnelles liées aux publicités de tiers, telles que la limitation de fréquence, l'historique financier, l'affiliation publicitaire, la détection de la fraude au clic, la recherche et l'analyse de marché, l'amélioration des produits et le débogage. Si certaines finalités opérationnelles peuvent certainement distinguer un utilisateur d'un autre, en principe, ces finalités ne justifient pas l'utilisation d'identifiants uniques. Ce point revêt une importance particulière dans le contexte des discussions actuelles concernant la mise en œuvre de la norme « Do Not Track » en Europe.

Cette analyse montre également que les cookies d'analyse d'origine ne sont pas exemptés de l'obligation de consentement, mais qu'ils présentent des risques limités pour le respect de la vie privée, pour autant que des protections suffisantes soient mises en place, notamment en proposant une information adéquate, la possibilité de se retirer facilement et des dispositifs d'anonymisation intégrale.

Enfin, pour décider si un cookie est exempté du principe du consentement informé, il importe de vérifier avec soin s'il remplit l'un des deux critères d'exemption définis à l'article 5, paragraphe 3, tel que modifié par la directive 2009/136/CE. Si, à l'issue de cette évaluation minutieuse, des doutes subsistent quant à l'applicabilité d'un critère d'exemption, les opérateurs de site web doivent examiner attentivement s'il n'est pas possible, dans la pratique, de recueillir le consentement des utilisateurs d'une manière simple et discrète, en évitant ainsi toute insécurité juridique.

Avis 02/2012 (WP 192) sur la reconnaissance faciale dans le cadre des services en ligne et mobiles

Ces dernières années ont été marquées par une croissance rapide de la disponibilité et de la précision de la technologie de reconnaissance faciale, qui été intégrée dans des services en ligne et mobiles à des fins d'identification, d'authentification/de vérification ou de catégorisation des personnes. Cette technologie est mise à la disposition d'organisations tant publiques que privées. Les réseaux sociaux et les téléphones intelligents offrent notamment des exemples de son utilisation dans les services en ligne et mobiles.

La capacité de collecter automatiquement des données et de reconnaître un visage à partir d'une image numérique a été examinée précédemment par le groupe de travail dans son document de travail sur la biométrie (WP80) et dans l'avis 03/2012 (WP193) sur les progrès des technologies biométriques. La reconnaissance faciale est envisagée dans le contexte de la biométrie étant donné que, bien souvent, elle contient suffisamment de détails pour rendre possible l'identification univoque d'une personne.

Dans cet avis, le groupe de travail a examiné le cadre juridique et formulé des recommandations appropriées applicables à la technologie de reconnaissance faciale utilisée dans le contexte des services en ligne et mobiles. Cet avis s'adresse aux autorités législatives européennes et nationales, aux responsables du traitement des données et aux utilisateurs de ces technologies, et s'inspire des principes auxquels il est fait référence dans l'avis 03/2012 dans le contexte des services en ligne et mobiles.

Le groupe de travail a conclu que les risques d'atteinte à la vie privée présentés par un système de reconnaissance faciale dépendent entièrement du type de traitement appliqué et des finalités, et a formulé des recommandations de meilleures pratiques concernant les principaux risques.

L'acquisition d'images en ligne ne peut se faire que sur une base juridique établie.

Les images numériques et les modèles devraient être utilisés uniquement dans le but spécifié pour lequel les images ont été fournies, et des contrôles techniques devraient être mis en place en vue de réduire le risque que les images numériques soient traitées ultérieurement par des tiers à des fins pour lesquelles l'utilisateur n'a pas marqué son consentement.

Les responsables du traitement des données doivent garantir la sécurité du transfert des données entre l'acquisition d'images et les autres stades de traitement (par ex., mise en ligne d'une image provenant d'un appareil photo sur un site web à des fins d'extraction des caractéristiques et de comparaison) en cryptant les canaux de communication ou l'image acquise elle-même.

Les responsables du traitement des données doivent veiller à ce que les données extraites d'une image numérique pour constituer un modèle ne contiennent que les informations requises aux fins spécifiées, de façon à éviter tout autre traitement éventuel. Les modèles ne devraient pas être transférables entre différents systèmes de reconnaissance faciale.

Étant donné que l'identification et l'authentification nécessiteront probablement le stockage du modèle à des fins de comparaison ultérieure, le groupe de travail a recommandé aux responsables du traitement des données de privilégier l'endroit le plus approprié pour le stockage des données, qu'il s'agisse de l'appareil de l'utilisateur ou des systèmes du responsable du traitement des données. Les responsables du traitement des données doivent garantir la sécurité des données conservées, en cryptant le modèle si nécessaire, de manière à ce qu'il soit impossible d'accéder sans autorisation au modèle ou à l'endroit où il est stocké. Lorsque la reconnaissance faciale est utilisée à des fins de vérification, des techniques de cryptage biométrique sont conseillées.

Enfin, le groupe de travail a recommandé que les responsables du traitement des données mettent à la disposition des personnes concernées des mécanismes appropriés pour exercer, le cas échéant, leur droit d'accès aussi bien aux images originales qu'aux modèles créés dans le contexte de la reconnaissance faciale.

1.3 RÉVISION DU CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES

Avis 01/2012 (WP 191) sur les propositions de réforme de la protection des données

D'une manière générale, le règlement apporte davantage de clarté. En ce qui concerne les personnes, le règlement renforce leurs droits, y compris par une transparence accrue, un plus grand contrôle du traitement, la minimisation des données, des dispositions particulières pour le traitement des données à caractère personnel concernant des enfants, un droit d'accès aux données renforcé, un droit d'opposition renforcé, le droit à la portabilité des données, un droit à la suppression des données renforcé (« droit à l'oubli numérique ») et un droit renforcé de recours devant les autorités chargées de la protection des données et devant les cours et tribunaux.

En ce qui concerne les responsables du traitement, le règlement apporte une simplification et une plus grande cohérence, un recentrage sur leur responsabilité à l'égard des données traitées et la nécessité de prouver cette responsabilisation par une protection des données dès la conception, une protection des données par défaut, des analyses d'impact sur le respect de la vie privée, la désignation d'un délégué à la protection des données, des obligations liées à la notification des violations de données et l'adoption de mesures de précaution à l'égard des transferts internationaux. En outre, les règles d'entreprise contraignantes sont expressément reconnues comme un outil permettant d'encadrer les transferts internationaux.

En ce qui concerne les sous-traitants, les obligations en matière de sécurité des données sont juridiquement fondées, et une obligation a été introduite pour que le sous-traitant endosse la responsabilité du responsable du traitement à l'égard d'une opération spécifique de traitement de données au cas où il outrepasserait les instructions du responsable du traitement à propos de ladite opération de traitement (ce qui présente un intérêt pour les prestataires « cloud »).

En ce qui concerne les autorités chargées de la protection des données, le règlement prévoit une indépendance et des pouvoirs renforcés, y compris des amendes administratives et l'obligation de consulter ces autorités à propos des mesures législatives, et il comprend des dispositions visant à garantir une application harmonisée de la législation et, au besoin, son application forcée, en particulier au moyen du « mécanisme de contrôle de la cohérence ».

Le groupe de travail émet de sérieuses réserves à l'égard de l'étendue du pouvoir conféré à la Commission pour adopter des actes délégués et des actes d'exécution, ce qui est tout particulièrement pertinent au vu du fait qu'il est question d'un droit fondamental, et du rôle de la Commission au sein du comité européen de la protection des données.

Le groupe de travail suggère qu'une évaluation approfondie indépendante soit réalisée concernant les coûts supplémentaires que cela représente pour les autorités chargées de la protection des données et le contrôleur européen de la protection des données (en tant que secrétariat du comité européen de la protection des données), sur la base des propositions actuelles.

Globalement, en ce qui concerne le projet de règlement, l'avis couvre les questions horizontales que sont, notamment, le rôle de la Commission, le rôle des autorités européennes chargées de la protection des données dans l'élaboration des politiques, les seuils pour les PME, les incidences sur les budgets et les ressources, les dispositions générales (*champ d'application, personnes concernées et données à caractère personnel, données biométriques, établissement principal, pseudonymisation, protection des données dès la conception et protection des données par défaut),* le principe du droit d'accès du public aux informations, l'utilisation ultérieure incompatible, les exceptions introduites pour les autorités publiques, les mineurs, le droit à l'oubli numérique, le marketing direct, le profilage, les représentants, la responsabilité, la notification des violations de données, le rôle et le fonctionnement des autorités chargées de la protection des données (*indépendance*, *pouvoirs*, *budget*, *marge d'appréciation),* la territorialité et la compétence des autorités chargées de la protection des données (guichet unique), l'assistance mutuelle, la cohérence (*application de la législation nationale (Chapitre IX)*, *délais),* le concept de « guichet unique » pour les personnes concernées, la structure institutionnelle du comité européen de la protection des données, les transferts internationaux, les divulgations non autorisées par la législation de l'UE, le droit à réparation et responsabilité, les amendes, les recours juridictionnels et les églises et associations religieuses.

Le groupe de travail prend note du choix explicite fait par la Commission européenne de ne pas présenter un instrument unique pour la protection des données dans tous les domaines, et de présenter une directive pour être l'instrument réglementant la protection des données dans le domaine de la police et de la justice pénale, au niveau élevé et constant visé par la Commission en la matière.

Le groupe de travail regrette que les dispositions portant sur les pouvoirs des autorités chargées de la protection des données ne soient pas très détaillées, ni cohérentes avec celles du règlement. Plus particulièrement, la directive ne comporte aucune disposition relative à l'accès aux locaux, contrairement au règlement. La capacité conférée à l'autorité de contrôle d'accéder aux locaux du responsable du traitement lorsque cela est nécessaire devrait s'appliquer à tous les secteurs.

Le groupe de travail regrette, dans la directive, l'absence de dispositions sur la fixation de délais, le contrôle et d'autres garanties, comme la limitation de l'utilisation des données pour les infractions graves, etc. Le groupe de travail note l'absence d'obligation, pour les autorités compétentes qui ont transmis des données, d'informer le destinataire que les données transmises étaient incorrectes ou avaient été transmises de manière illicite.

Pour finir, le groupe de travail regrette que la directive ne comporte aucune disposition sur le transfert vers des entités privées ou d'autres autorités qui ne sont pas considérées comme des autorités compétentes

au titre de la directive. Dès lors, le groupe de travail demande instamment au législateur européen d'introduire une disposition autorisant le transfert de données de nature répressive vers des entités privées uniquement dans des circonstances strictement définies par la législation.

En ce qui concerne la directive, les sujets traités sont le choix de l'instrument, la cohérence, le champ d'application, les principes de traitement des données, les droits des personnes concernées, les obligations des responsables du traitement, les transferts internationaux (*principes généraux applicables aux transferts et aux transferts ultérieurs, décisions négatives relatives au caractère adéquat du niveau de protection, transferts moyennant des garanties appropriées* et *dérogations)* et les pouvoirs des autorités chargées de la protection des données et la coopération.

Avis 08/2012 (WP 199) apportant des contributions supplémentaires au débat sur la réforme de la protection des données

Dans son avis du 23 mars 2012, le groupe de travail « Article 29 » a présenté sa première réaction générale face aux propositions de la Commission et mis en évidence des sujets de préoccupation ainsi qu'un certain nombre de suggestions en vue d'améliorer ces propositions. En vue des discussions actuelles et à venir au Parlement européen et au Conseil, le groupe de travail a décidé d'adopter cet avis qui fournit des indications supplémentaires, notamment sur certains concepts clés en matière de protection des données, et analyse la nécessité et les effets de la proposition d'actes délégués, en proposant, là où cela s'avère nécessaire, des alternatives plus appropriées.

Les concepts clés en étaient la définition des données à caractère personnel et la notion de consentement.

Sur les actes délégués proposés, le groupe de travail a exprimé son avis sur la nécessité ou non de ces actes en faisant référence à des dispositions spécifiques de la proposition.

En ce qui concerne l'article 14, paragraphe 7, qui vise à préciser davantage les divers critères de classification dans les catégories de destinataires, les exigences de notification d'un accès potentiel, les informations complémentaires pour des circonstances et secteurs particuliers et les conditions et les garanties appropriées concernant les exceptions, le groupe de travail a accepté que ces conditions pourraient être établies par un acte délégué, tout en soulignant que des indications plus détaillées de la part du comité européen de la protection des données permettraient de pouvoir mieux déterminer les cas dans lesquels les responsables du traitement pourraient faire usage de la dérogation en partant d'une analyse de circonstances diverses et de contextes concrets.

En ce qui concerne l'article 15, paragraphe 3, qui vise à préciser davantage les critères et les exigences applicables à la communication à la personne concernée du contenu des données à caractère personnel faisant l'objet d'un traitement, et de toute information disponible sur l'origine de ces données, aucune législation ou orientations supplémentaires n'ont semblé nécessaires.

Concernant l'article 17, paragraphe 9, qui vise à préciser les exigences et les critères relatifs au droit à l'oubli dans des secteurs spécifiques ou des circonstances spécifiques de traitement de données et les conditions présidant à la suppression des liens vers des données à caractère personnel, à la copie ou à la reproduction de ces données dans le cadre de services de communication accessibles au public, le groupe de travail a estimé qu'un acte délégué semblait effectivement être le moyen le plus indiqué, pour autant qu'il soit adopté au moment de l'entrée en vigueur du règlement. La même conclusion s'applique à l'article 20, paragraphe 5, qui vise à préciser davantage les critères et conditions applicables aux mesures nécessaires pour sauvegarder les intérêts légitimes de la personne concernée, si le comité européen de la protection des données fournit des orientations supplémentaires.

Il n'a pas été jugé nécessaire de fournir des orientations supplémentaires dans un acte délégué pour les articles 8 (exigences relatives au consentement), 12 (demandes excessives et frais), 22 (« l'article de la responsabilité générale »), 26 (choix d'un sous-traitant), ou 28 (conservation d'une trace documentaire des traitements).

Des orientations fournies par le comité européen de la protection des données ont été considérées comme l'option à privilégier pour préciser davantage les critères et exigences visés aux articles 6 (base juridique), 9 (données sensibles), 23 et 30 (sécurité du traitement) et 34 (contrôle préalable).

Eu égard à leur importance pour toutes les parties intéressées, il conviendrait de traiter des critères et exigences des articles 31 et 32 (obligation de notifier une violation de données à caractère personnel), ainsi que de l'article 83, dans le texte du règlement proprement dit, au moins dans les grandes lignes. Pour certaines précisions, un acte délégué conviendrait, pour autant qu'il soit adopté au plus tard lors de l'entrée en vigueur du règlement.

Des actes délégués, accompagnés d'une orientation supplémentaire fournie par le comité européen de la protection des données, ont été jugés comme une solution appropriée pour spécifier les critères et les exigences des articles 33, 35, 37 et 44, paragraphe 1, point h.

Les actions visées aux articles 39 (certification), 79 (amendes), 81 et 82 (actes délégués) ont été considérées comme suffisantes.

1.4. DONNÉES À CARACTÈRE PERSONNEL

1.4.1 epSOS

Document de travail 01/2012 (WP 189) sur epSOS

Ce document de travail du groupe de travail « Article 29 » est destiné à donner des orientations sur les questions relatives à la protection des données dans le cadre du projet epSOS (European Patients Smart Open Services), à clarifier les principes les plus importants de la directive 95/46/CE et à expliquer la manière dont le document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (WP 131), s'applique au projet epSOS.

EpSOS est un projet pilote à grande échelle, qui concerne les systèmes de dossiers médicaux électroniques dans le contexte de deux services transfrontaliers : le dossier du patient et la prescription en ligne.

Dans son évaluation, le groupe de travail est arrivé à plusieurs conclusions.

Toutes les données contenues dans les documents médicaux, les dossiers médicaux électroniques et les systèmes de DME sont à considérer comme des « données à caractère personnel sensibles » et relèvent dès lors de l'article 8 de la directive. Le traitement de données relatives aux soins de santé doit reposer sur une base juridique précise.

L'une des conditions de validité du consentement est que la personne concernée ait reçu des informations satisfaisant aux exigences des articles 10 et 11 de la directive.

Le traitement des données à caractère personnel doit être strictement limité au minimum nécessaire à la réalisation des finalités d'epSOS, qui doivent être spécifiées, explicites et légitimes. Afin de garantir que les données ne soient pas conservées plus longtemps que nécessaire dans le système epSOS, il convient de fixer une durée de conservation maximale, ainsi qu'une procédure commune précisant le sort réservé aux données à la fin de cette période de conservation.

Toute demande d'accès aux données à caractère personnel disponibles via le système epSOS devrait reposer sur l'existence d'une nécessité réelle de consulter des données spécifiques liées aux soins ou au traitement médical à fournir ou aux médicaments à prescrire ou à délivrer dans un cas particulier.

Étant donné le caractère transfrontalier des activités d'epSOS, la coopération entre les autorités chargées de la protection des données pour contrôler le projet epSOS est fortement recommandée.

Tous les responsables du traitement des données qui manipulent des données d'epSOS doivent adresser une notification à leur autorité de contrôle compétente conformément à la législation nationale applicable, que la personne concernée soit un ressortissant national ou qu'elle réside dans un autre État

membre, y compris si les données en question proviennent de responsables du traitement se trouvant dans d'autres États membres.

Un niveau élevé de sécurité informatique est nécessaire pour epSOS et, notamment, ce qui suit : tout le personnel prenant part à la mise en œuvre du projet devrait recevoir des instructions écrites précises expliquant comment utiliser correctement le système epSOS pour éviter les risques et les atteintes à la sécurité ; des mécanismes appropriés devraient être prévus pour l'utilisation des systèmes de stockage et d'archivage des dossiers de patients et des prescriptions en ligne afin de protéger les données contre les accès non autorisés, le vol ou la perte totale/partielle des supports d'enregistrement ; pour les échanges de données, des protocoles de communication sécurisés et le cryptage de bout en bout doivent être adoptés sur la base des normes de cryptage pour sécuriser les communications électroniques ; il convient d'accorder une attention toute particulière à l'adoption d'un système d'identification électronique fiable et efficace permettant une authentification sûre (tant pour les membres du personnel participants que pour les patients) ; le système doit être capable d'enregistrer et de retracer correctement, de façon contrôlable, les différentes opérations que comprend le traitement des données ; les accès ou modifications de données non autorisés doivent être empêchés lors du transfert ou de l'enregistrement des données de sauvegarde (par exemple, au moyen du cryptage) ; en ce qui concerne le système de prescription en ligne, des mesures supplémentaires devraient être adoptées pour garantir que les opérateurs pharmaceutiques ne puissent accéder aux prescriptions numériques que pour délivrer les médicaments prescrits ; dans les situations d'urgence, tout accès devrait être consigné et soumis à un audit.

Tous les responsables du traitement des données qui manipulent des données d'epSOS doivent donner aux personnes concernées un droit d'accès à leurs données et un droit de rectification, d'effacement et de verrouillage de ces données, et une personne concernée devrait pouvoir poser des questions sur l'accès et demander la rectification, l'effacement ou le verrouillage des données à n'importe quel responsable du traitement ou à tout autre organisme intervenant dans l'échange d'informations dans le cadre du projet epSOS. Une demande d'accès ou une demande de rectification, d'effacement ou de verrouillage des données adressée à un partenaire epSOS qui ne manipule pas les données du demandeur devrait être renvoyée au responsable du traitement compétent au sein du système epSOS, même si ce dernier se trouve dans un autre État membre.

Le projet epSOS devrait prévoir la possibilité de donner aux personnes concernées un accès (électronique) direct à leurs propres données aux fins de lecture. Il conviendrait de créer un site web epSOS commun précisant les droits spécifiques conférés aux personnes concernées par les législations de tous les États participants.

1.4.2 Évolution des technologies biométriques

Avis 3/2012 (WP193) sur l'évolution des technologies biométriques

Dans le document de travail sur la biométrie de 2003 (WP80), le groupe de travail s'était penché sur les questions de protection des données liées à l'utilisation des nouvelles technologies qui permettaient de lire et de traiter les données biométriques par voie électronique.

Dans les années qui ont suivi, l'utilisation de ces technologies s'est généralisée et plusieurs nouveaux services ont été mis en place. Les technologies biométriques qui nécessitaient auparavant d'importantes ressources financières ou informatiques sont devenues bien plus rapides et moins onéreuses. Ces technologies sont étroitement liées à certains traits d'une personne, dont certains peuvent être utilisés pour révéler des données sensibles. Par ailleurs, bon nombre d'entre elles permettent le pistage, le suivi ou le profilage automatisés de personnes et, partant, peuvent avoir un impact considérable sur la vie privée et le droit des personnes à la protection des données.

Cet avis a pour but de fournir un cadre révisé et actualisé pour des directives et des recommandations générales unifiées sur la mise en œuvre des principes de protection des données et de la vie privée dans des applications biométriques. Il s'adresse aux autorités législatives nationales et européennes, à l'industrie des systèmes biométriques et aux utilisateurs de ces technologies.

Les systèmes biométriques reposent sur plusieurs acteurs : fabricants, intégrateurs, revendeurs, installateurs, clients et personnes concernées. La sécurité doit être une préoccupation centrale car les données biométriques sont irrévocables. Le groupe de travail recommande un niveau élevé de protection technique pour le traitement des données biométriques, grâce à l'utilisation des dernières techniques. À cet égard, le groupe de travail recommande de suivre les normes de l'industrie concernant la protection des systèmes dans lesquels les données biométriques sont traitées.

Le respect de la vie privée dès la conception est le concept qui consiste à intégrer de manière proactive la vie privée dans la technologie elle-même. Ce concept concerne l'ensemble de la chaîne de valeur des systèmes biométriques. Le groupe de travail recommande que les systèmes biométriques soient conçus en suivant des « cycles de développement » officiels qui se décomposent comme suit : spécification des exigences sur la base d'une analyse des risques et/ou d'une évaluation spéciale de l'impact sur la vie privée ; description et justification de la manière dont le projet répond aux exigences ; validation par le biais de tests fonctionnels et de sécurité ; et vérification du respect du cadre réglementaire du projet final.

L'évaluation de l'impact sur la vie privée est un processus en vertu duquel un organisme réalise une évaluation des risques liés au traitement des données à caractère personnel et définit des mesures supplémentaires pour atténuer ces risques. Cette évaluation doit tenir compte de la nature des informations collectées, de la finalité des informations collectées, de la précision du système, de la base juridique et du respect des lois, de l'accès au dispositif et de l'échange interne et externe d'informations par le responsable du traitement, qui impliqueront des techniques et procédures de sécurité pour protéger des données à caractère personnel d'un accès non autorisé, des mesures les moins invasives dans la vie privée déjà adoptées, des décisions prises concernant la période de conservation et la suppression de données et des droits de la personne concernée.

Les données biométriques requièrent une attention particulière car elles identifient sans ambiguïté une personne en utilisant ses caractéristiques comportementales ou physiologiques uniques. C'est pourquoi l'évaluation de l'impact sur la vie privée doit viser à évaluer la manière dont l'usurpation d'identité, le détournement de la finalité et la violation de données peuvent être évités ou fortement limités par le système qu'elle analyse.

Le traitement des données biométriques, en raison de leur nature, requiert des précautions et des mesures techniques et organisationnelles spéciales pour éviter des effets indésirables pour la personne concernée en cas de violation de données.

Les mesures techniques, surtout en cas d'utilisation de larges bases de données biométriques, pourraient inclure l'utilisation de modèles biométriques, le stockage sur un dispositif personnel plutôt que le stockage centralisé, la capacité de renouvellement et la révocabilité des liens d'identité, la forme cryptée, la lutte contre la mystification, le cryptage et le décryptage biométriques, et les mécanismes d'effacement automatique des données.

Les mesures organisationnelles pourraient prévoir que le responsable du traitement établisse une procédure claire pour savoir qui peut accéder aux informations dans le système, si l'accès est partiel ou non, et assurer un suivi de toutes les actions.

Chapitre Deux
Principaux développements au sein des États membres

ALLEMAGNE

A. Résumé des activités et actualités :

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

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

Organisation	Commissaire fédéral à la protection des données et à la liberté d'information
Président et/ou collège	Peter Schaar, commissaire fédéral
Budget	9 125 000 EUR
Personnel	86 Protection des données : 82 ; Liberté d'information : 4
Activités générales	
Décisions, avis, recommandations	s. o.
Notifications	s. o.
Examens préalables	s. o.
Demandes émanant des personnes concernées	8 173
Plaintes émanant des personnes concernées	4 568
Conseils sollicités par le Parlement ou le gouvernement	s. o.
Autres renseignements relatifs aux activités générales	s. o.
Activités d'inspection	
Contrôles, enquêtes	s. o.
Activités de sanction	

Sanctions	s. o.
Amendes	cf. TB 2012 – s. o.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

1) La Cour fiscale fédérale considère que le numéro d'identification fiscale est compatible avec le droit fondamental à l'autodétermination informationnelle

La Cour fiscale fédérale (BFH) a jugé que le numéro d'identification fiscale, lancé en 2008, est constitutionnel dans la mesure où l'intérêt public à bénéficier d'un régime fiscal cohérent justifie une infraction du droit à l'autodétermination informationnelle (BFH, arrêt du 18 janvier 2012, II R 49/10), même si les principes de finalité et de nécessité doivent être strictement respectés. La législature n'est par conséquent pas libre d'étendre l'utilisation du numéro d'identification fiscale comme elle le souhaite, en raison des limites strictes qui découlent des exigences applicables en termes de protection des données, également définies par la Section 139b(2) à (5) du Code fiscal. La Cour constitutionnelle fédérale n'ayant pas encore eu l'opportunité de se prononcer sur la constitutionnalité du numéro d'identification fiscale, la décision finale en la matière reste en suspens.

2) L'arrêt de la Cour constitutionnelle fédérale concernant le fichier antiterroriste (1 BvR1215/07 du 24 avril 2013) revêt une importance fondamentale. Il contient notamment les déclarations suivantes :

I. La Cour Européenne de Justice n'est pas le tribunal compétent au sens de l'article 101(1) de la loi fondamentale pour les questions exclusivement liées aux droits de base allemands. L'applicabilité des droits fondamentaux européens est exclue d'emblée si une loi nationale poursuit des objectifs spécifiques qui ne peuvent qu'indirectement affecter le fonctionnement des relations juridiques ordonnées en vertu du droit de l'Union. Dans ces cas, il n'est nul besoin qu'une décision préjudicielle au titre de l'article 267 TFUE clarifie le niveau de protection des droits fondamentaux en vertu du droit de l'Union.

II. Le principe de séparation informationnelle découle du droit fondamental à l'autodétermination informationnelle. Par conséquent, les données ne peuvent généralement pas être partagées entre les services de renseignements et les autorités policières. Les restrictions ne sont autorisées qu'en des circonstances exceptionnelles. L'échange de données entre services de renseignements et autorités policières pour de possibles déploiements opérationnels doit généralement servir un intérêt public supérieur qui justifie un accès aux informations dans les conditions simplifiées autorisées aux services de renseignements.

III. La collecte et le traitement de données de contact ne sont autorisés qu'en vertu de conditions très restrictives (que la personne concernée en ait conscience ou non).

IV. Le responsable doit également documenter en détails et divulguer les critères internes de prise de décision et de classification (à des fins de contrôle par le responsable de la protection des données).

V. Les contrôles de supervision, y compris par les responsables de la protection des données, revêtent une importance cruciale et offrent un soutien légal aux droits subjectifs que les tribunaux font respecter. Un système de contrôles de supervision inadéquat d'un point de vue légal et/ou de fait peut justifier une interférence disproportionnée avec le droit de la personne concernée à l'autodétermination

informationnelle. Les principales conditions préalables pour une supervision efficace comprennent l'existence d'autorités de supervision dotées de pouvoirs effectifs, l'enregistrement exhaustif des accès et modifications apportées aux données, et la capacité de récupérer les données dans la pratique, qui doit être assurée par des mesures techniques et organisationnelles.

VI. Les responsables de la protection des données sont autorisés à coopérer et à se soutenir mutuellement, via une assistance administrative, par exemple, par le biais d'une délégation ou d'une autorisation dans l'exercice de leurs pouvoirs. Une interaction solide entre les différentes autorités de supervision doit également être maintenue dans la pratique.

VII. Des contrôles obligatoires réguliers définis par le droit, qui doivent pour le moins être exécutés tous les deux ans, sont également nécessaires à une supervision efficace.

VIII. La législature est incitée à vérifier et, si nécessaire, amender les règlements existants en matière de transmission de données afin de préserver ces principes.

3) Décision de la Cour constitutionnelle fédérale sur le stockage et l'utilisation de données de télécommunications

Dans une décision du 24 janvier 2012, la Cour constitutionnelle fédérale a jugé que toute demande de données de télécommunications devait toujours être justifiée et faire l'objet d'une autorisation de transmission des données (on parle alors de « modèle à double entrée »). C'est la raison pour laquelle le stockage et la transmission des données de télécommunications aux autorités en charge des enquêtes ont été déclarés non constitutionnels et interdits, ces autorités ayant préalablement bénéficié d'un accès aux mots de passe et codes PIN. Par conséquent, les autorités en charge des enquêtes étaient jusqu'ici à même d'accéder à des téléphones mobiles saisis et de procéder à des recherches parmi les données enregistrées sans qu'il soit établi avec certitude qu'elles en avaient le droit.

Le Tribunal constitutionnel fédéral a également jugé qu'une demande d'informations sur les abonnés d'une adresse IP dynamique constituait une violation du secret des télécommunications. Pour identifier une adresse IP dynamique, les sociétés de télécommunications doivent inspecter les données d'appels de leurs clients, ce qui implique d'accéder à des télécommunications spécifiques soumises à la protection prévue par l'Article 10 de la Loi fondamentale. La législature allemande doit ici établir une disposition claire visant à garantir la protection des données extrêmement sensibles sur le trafic des télécommunications.

C. Autres informations importantes

FATCA

La loi FATCA (Foreign Account Tax Compliance Act), qui est entrée en vigueur en mars 2010, est une loi américaine relative à la collecte des actifs des comptes bancaires à l'étranger (en dehors des États-Unis) des personnes et sociétés imposables aux États-Unis. La FATCA repose essentiellement sur des obligations de notification et de compte rendu renforcées pour les banques et autres établissements financiers à l'étranger (Foreign Financial Institutions – FFIs) envers les autorités fiscales américaines (Internal Revenue Service – IRS). De substantielles retenues à la source peuvent être imposées en cas de non respect des obligations de notification et de compte rendu.

La mise en œuvre de la FATCA a soulevé d'importants problèmes de protection des données. Par exemple, la question a été soulevée de savoir si les transmissions à l'IRS étaient sujettes aux règles juridiques prévues aux Sections 4b et 4c de la loi fédérale sur la protection des données (BDSG) ou au seul consentement. Pour y répondre, la France, l'Italie, l'Espagne, le Royaume-Uni et l'Allemagne se sont entendus avec les États-Unis sur un modèle d'accord conçu pour servir de base aux accords bilatéraux.

Le modèle d'accord a été présenté le 26 juillet 2012. Dans ce modèle, les cinq pays s'engagent à collecter les informations sur les comptes bancaires détenus par des clients américains au sein d'établissements financiers domiciliés sur leurs territoires et à les transmettre aux autorités américaines. En retour, les États-Unis acceptent d'exempter l'ensemble des établissements financiers des signataires respectifs du traité de l'exigence de conclusion d'accords avec l'IRS. Ce modèle d'accord crée un cadre pour les comptes rendus des données de comptes bancaires par les établissements financiers à leurs autorités fiscales nationales respectives et l'échange subséquent des données respectives dans le cadre des traités bilatéraux de double imposition existants.

L'accord FATCA (accord en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et de mettre en œuvre la loi américaine relative au respect des obligations fiscales concernant les comptes étrangers, dite « Loi FATCA ») entre les États-Unis et l'Allemagne a été signé par les représentants de la République fédérale d'Allemagne et les États-Unis le 31 mai 2013 et a été ratifié par une loi du Parlement. Cet accord repose essentiellement sur le modèle d'accord susmentionné du 26 juillet 2012.

Lors des négociations, le Commissaire fédéral à la protection des données et à la liberté d'information (BfDI) a fait campagne en faveur des exigences de base de la législation sur la protection des données. Cette campagne a notamment porté sur la création d'une règle permissive pour les établissements financiers en vertu de la loi sur la protection des données, spécifiant l'utilisation prévue des données à caractère personnel transmises et normalisant les garanties procédurales et organisationnelles.

Contrairement à l'incitation du BfDI, toutefois, les garanties procédurales et les mesures de sécurité des données techniques et organisationnelles sont réglementées dans le cadre d'un simple accord de mise en œuvre du traité.

L'accord FATCA envisage désormais une restriction sur l'utilisation et une assurance de confidentialité pour les données destinées à être utilisées. Le BfDI a également recommandé qu'une règle permissive soit créée pour les établissements financiers auxquels il est demandé d'envoyer des informations par l'inclusion de la Section 117c du Code fiscal allemand (AO), qui prévoit, en matière de traitement de données, des restrictions sur les principes de limitation de l'utilisation des données et de nécessité. Les établissements financiers allemands disposent par conséquent d'une disposition permettant la transmission de données.

Les obligations des établissements financiers doivent être définies en détails par un instrument légal basé sur la Section 117c du Code fiscal allemand.

AUTRICHE

A. Résumé des activités et actualités

Sur la période de référence, le Parlement a adopté la **loi d'amendement de la juridiction administrative 2012**. ([2]) Cet amendement de la loi constitutionnelle fédérale (B-VG) prévoit la dissolution de certaines autorités administratives autonomes (dont la Commission de protection des données) fin 2013, et le transfert de leurs activités judiciaires vers des tribunaux administratifs nouvellement créés. Dans le cas de la Commission de protection des données, ce transfert n'était pas possible sous cette forme, dans la mesure où l'article 28 de la directive 95/46/CE stipule que, lorsque la Commission de protection des données est dissoute, une nouvelle autorité de protection des données doit être établie et les tâches de la Commission de protection des données doivent lui être transférées. Un amendement correspondant de la loi sur la protection des données de 2000 (ou « Amendement 2014 de la DSG ») ([3]) envisage par conséquent la création d'une **autorité monocratique de protection des données** qui remplacera 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.

Pendant la période de référence, la « **Loi sur les dossiers médicaux électroniques » (ELGA-G)** a été adoptée. Le document de travail WP 131 du groupe de travail « Article 29 » sur le traitement des données des patients contenues dans les dossiers médicaux électroniques (DME) de 2007, dont de larges pans sont intégrés à la loi, a joué un rôle important dans la création de celle-ci. La loi envisage toutefois un système universel de refus (en partie inspiré du système décrit au WP 131, et gradué en fonction de la sensibilité des données).

À l'occasion de la **Journée européenne de la protection des données 2012**, un événement, déjà érigé au rang de tradition et principalement consacré au nouveau **paquet de propositions pour la protection des données de l'UE,** a été organisé avec le Conseil de la protection des données et la Chancellerie fédérale. Cet événement a eu lieu peu après la présentation par la Commission européenne des projets de règlement de base sur la protection des données et de directive sur la coopération policière et judiciaire en matière pénale, et a par conséquent pris une tournure très thématique.

Pendant la période de référence, **l'arrêt rendu par la Cour de justice européenne sur l'indépendance de l'autorité de supervision** en Autriche ([4]) a rejeté les arguments de la République d'Autriche aux motifs que la Commission de protection des données n'était pas suffisamment indépendante. Pour résumer, la Cour a jugé que le bureau de la Commission de protection des données était trop proche de la Chancellerie fédérale et a exprimé ses doutes quant à la position du membre administrateur (qui présente, pour le moins, une apparence de dépendance vis-à-vis de la Chancellerie fédérale) et au caractère excessif des exigences de compte rendu de la Commission de protection des données vis-à-vis du Chancelier fédéral. ([5])

Organisation	Commission autrichienne de la protection des données
Président et/ou collège	Président : Dr Anton SPENLING Membre administrateur : Dr Eva SOUHRADA-KIRCHMAYER

([2]) BGBl. I 51/2012.

([3]) BGBl. I n° 83/2013.

([4]) ECJ 16.10.2012, affaire C-614/10, Commission / Autriche.

([5]) C'est en réponse à cet arrêt que la législature a adopté « l'amendement DSG 2013 », BGBl. I n° 57/2013, qui établit la Commission de protection des données en tant qu'autorité et unité du personnel distincte.

	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 2012. Les dépenses sont couvertes par le budget de la Chancellerie fédérale.
Personnel	Jusqu'en novembre 2012 : 20,65 postes à temps plein (16 temps pleins et 8 temps partiels), depuis mi-novembre 2012 : 21,65 postes.
Activités générales	
Décisions, avis, recommandations	149 décisions formelles (plaintes), 246 dossiers déposés auprès du Médiateur, 2 recommandations et 61 autorisations (transfert de données vers des pays tiers, recherche et enquêtes).
Notifications	6 197
Examens préalables	3 393
Demandes émanant des personnes concernées	Par écrit : 940 Par téléphone : aucune documentation écrite
Plaintes émanant des personnes concernées	Plaintes ayant mené à une décision formelle : 149 Plaintes ayant mené à un éclaircissement ou à une recommandation : 246
Conseils sollicités par le Parlement ou le gouvernement	Cette fonction relève de la compétence de deux autres institutions : le « Datenschutzrat » (conseil de la protection des données) et le service juridique du gouvernement, qui dépend de la Chancellerie fédérale.
Autres renseignements relatifs aux activités générales	125 millions d'identifiants spécifiques à des secteurs ont été émis, plus de 5 000 nouvelles personnes et environ 1,1 million de nouvelles personnes morales ont été inscrites au registre des identités électroniques 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. Elle est également chargée de contrôler ce système de gestion.
Activités d'inspection	
Contrôles, enquêtes	22, la plupart en matière de vidéosurveillance.
Activités de sanction	
Sanctions	Aucune. La DPA autrichienne ne peut imposer de sanctions.

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

B. Jurisprudence

1. Caméra vidéo sur un véhicule

Pendant l'année de référence, l'enregistrement d'une application de données de « *vidéosurveillance à des fins de protection de l'objet surveillé (le véhicule privé de l'utilisateur situé dans les environs immédiats) ou de respect des obligations légales de diligence, obtention d'éléments de preuve comprise, avec extraction exclusive dans la situation définie par les fins désignées, sous réserve que les faits spécifiques justifient la présomption que l'objet surveillé puisse être la cible ou le lieu d'une attaque dangereuse* » a été rejeté par la Commission de protection des données.

Le demandeur avait demandé à entrer cette application de données dans le registre de traitement des données tenu par la Commission de protection des données en tant qu'application de vidéosurveillance (Sections 50a et suivantes, DSG 2000). Le déclarant a nommé « les autorités ou le tribunal compétent (pour la remise de preuves en matière pénale) », les « autorités de sécurité (à des fins de maintien de la paix) », les « tribunaux (pour la remise de preuves en matière civile) » et les « sociétés d'assurance (pour le règlement des cas d'assurance) » comme étant les destinataires prévus des transmissions. Invité à faire part de ses commentaires, le demandeur a déclaré que l'application était uniquement destinée à des fins privées (comme les caméras vidéo sur Kärntner Strasse ou les athlètes portant des caméras sur leur casque), c'est-à-dire des fins autres que commerciales ou non privées. Il ne s'agissait pas de vidéosurveillance au sens de l'enregistrement systématique et continu d'événements liés à un objet ou à une personne spécifique. Le cas échéant, les enregistrements auraient néanmoins pu servir à poursuivre des actes criminels. Aucun objet spécifique n'était destiné à être enregistré. Les enregistrements privés peuvent être conservés pour une durée illimitée, et les données ne font l'objet d'aucun écrasement cyclique.

Dans les motifs de son rejet, la Commission de protection des données a déclaré que l'application de données en question devait être considérée comme un système de vidéosurveillance impliquant l'enregistrement systématique (de chaque déplacement ou, pour le moins, de types de déplacement spécifiques) et continu (du trajet complet) d'événements (le trafic routier autour du véhicule), lié à un objet spécifique (le véhicule de l'utilisateur) ou à une personne spécifique (au moins le conducteur du véhicule). Il ne s'agissait donc pas d'une utilisation exclusive de données à des fins personnelles ou familiales. Dans ce cas, la surveillance du trafic et de l'environnement dans lequel se trouve un véhicule était caractérisée par l'intention manifeste de générer des preuves en vue d'une possible transmission aux autorités chargées des enquêtes pénales, aux tribunaux, etc. Cette intention était contraire à l'idée d'utilisation « exclusive » à des fins privées. Par ailleurs, le demandeur n'avait pas les « compétences légales » ni « l'autorité légale » d'exercer des activités de vidéosurveillance dans un lieu public. Compte tenu du monopole de l'État sur l'exercice du pouvoir, seules les autorités de sécurité sont autorisées à exercer des activités de vidéosurveillance dans des lieux publics, et leur juridiction est basée sur les exigences de la loi autrichienne sur la sécurité intérieure.

2. Dans une recommandation, la Commission de protection des données a invité une société à éviter que l'acceptation de ses Conditions générales (et, par conséquent, la conclusion du contrat correspondant) ne dépende de celle d'une clause de consentement qui y était incluse.

L'intervenant a déclaré que la société utilisait une clause de consentement de ses Conditions générales (CG) afin d'obtenir le consentement de clients pour l'utilisation de leurs données dans le cadre de concours et d'activités de collecte de fonds. Par conséquent, l'intervenant a estimé que son droit à la confidentialité avait été enfreint, puisqu'il avait été obligé, par l'inclusion de cette déclaration de consentement aux CG, d'accepter les applications de données mentionnées dans les CG.

La Commission de protection des données a été incitée à initier des procédures en vertu de la Section 30 DSG 2000 (procédure de contrôle et de médiation). La société a maintenu que cette déclaration de consentement devait être considérée comme « volontaire » malgré son inclusion aux CG, dans la mesure où l'offre sous-jacente à la déclaration de consentement représentait l'achat volontaire d'un produit, auquel la personne concernée était libre de procéder. Par conséquent, la déclaration de consentement liée à l'achat du produit n'était selon elle pas une contrainte.

La Commission de protection des données (citant divers commentaires ainsi que l'avis 15/2011 sur la définition du « consentement » au sens de la directive 95/46/CE sur la protection des données adopté par le groupe de travail « Article 29 », WP 187) a conclu qu'en l'espèce, il n'était pas possible pour le client de conclure le contrat souhaité avec la société sans également accepter la clause de consentement incluse aux CG. La Commission de protection des données a jugé cette impossibilité incompatible avec l'exigence de consentement volontaire définie aux Sections 4 n° 14 DSG 2000 et 8(1) n° 2 DSG 2000. Le client devrait au contraire bénéficier de l'opportunité de conclure le contrat souhaité sans avoir à soumettre la déclaration de consentement (la solution « de refus »), en concevant les CG, par exemple, de telle manière que la déclaration de consentement doive être cochée de manière distincte.

BELGIQUE

A. Résumé des activités et actualités

D'un point de vue législatif, l'année 2012 a notamment été marquée par quatre développements majeurs. Le décret du 13 juillet 2012 adopté par le parlement régional flamand portant création et organisation d'un intégrateur de services flamand (ISF) est le premier d'entre eux. L'ISF y est défini comme l'instance qui par ou en vertu d'une loi (fédérale ou régionale) est chargée de l'organisation de l'échange électronique de données entre différentes instances relevant de l'administration flamande et de l'accès intégré aux données. Toute communication vers et au départ de l'ISF doit, sauf exceptions, être autorisée par la Commission de contrôle flamande (Vlaamse Toezichtcommissie) en place depuis 2010. Une législation fédérale a également reconnu et organisé un intégrateur de services fédéral (FEDICT). L'article 7 de la loi concernée est particulièrement important pour le fonctionnement de la Commission de la protection de la vie privée (CPVP) puisqu'il lui confie une mission de coordination dans l'octroi des éventuelles autorisations à délivrer par différents comités sectoriels et celle d'indiquer quel est le comité chargé de délivrer cette autorisation, après avis des autres comités sectoriels compétents. La loi du 3 août 2012 relative aux traitements de données à caractère personnel réalisés par le Service Public Fédéral Finances (SPF Finances) dans l'exercice de ses missions est le fruit du dialogue noué entre la CPVP et ledit SPF, dialogue mu par la ferme volonté de la CPVP de voir consacrés les principes de base de la protection des données lors d'échanges interdépartementaux et avec d'autres instances externes. Dans une première version, cette législation dérogeait dans une large mesure et de manière générale au droit d'accès consacré par l'article 10 de la Loi vie privée (LVP) en cas d'enquête relative à un contribuable. Suivant l'avis défavorable de la CPVP sur cette restriction, la loi a été modifiée et prévoit aujourd'hui un examen au cas par cas de la question de savoir si l'exercice d'un droit d'accès nuirait ou non à l'enquête en cours. Le cas échéant, la restriction au droit d'accès fera l'objet d'une décision individualisée et motivée. La modification du Code de déontologie journalistique établissant désormais clairement que des informations tirées des médias sociaux tels Facebook ne peuvent être utilisées par les médias dans leurs publications sans le consentement explicite des personnes concernées est également le résultat d'un long dialogue avec la CPVP. L'émotion suscitée par l'accident de car de Sierre en mars 2013 à la suite duquel certaines images (d'enfants principalement) issues de ces médias sociaux ont été publiées par la presse a très certainement permis d'aboutir. Enfin, au titre de quatrième développement législatif à mentionner figure l'adaptation de la législation relative aux communications électroniques, transposant en droit belge la directive relative aux cookies et ce, après une recommandation et un avis de la CPVP. Parmi les autres avis et recommandations adoptés par cette dernière, épinglons celui relatif à la mise en place du principe des sources authentiques, d'une banque — carrefour d'échange de données et d'une « Commission vie privée Wallonie-Bruxelles » en Région wallonne et Communauté française, homologue de la Commission de contrôle flamande précédemment évoquée. Dans sa Recommandation « Cybersurveillance » relative au contrôle patronal de l'utilisation par les travailleurs de moyens de communication électroniques sur le lieu de travail, plus précisément le courriel et Internet, la CPVP propose une manière équilibrée de concilier le respect dû à la protection de la vie privée et des données à caractère personnel des travailleurs d'une part et celui dû aux prérogatives patronales et au bon fonctionnement de l'entreprise d'autre part (voir aussi le rapport 2011).

Réforme européenne de la protection des données

Enfin, l'avis d'initiative de la CPVP sur le projet de règlement européen déposé par la Commission européenne en début d'année épingle les nombreuses et épineuses questions ainsi que les fermes oppositions que suscitent tant le choix de l'instrument que le contenu de ce projet de réforme du cadre règlementaire de la protection des données dans l'Union européenne aux yeux de la CPVP ; il matérialise l'important travail d'analyse de ce texte réalisé au cours de l'année 2012.

Pour le surplus, l'ensemble des activités de la CPVP est repris dans son Rapport annuel 2011 disponible à l'adresse : http://www.privacycommission.be/sites/privacycommission/files/documents/rapport-annuel-2012.pdf

Organisation	Commission de la protection de la vie privée
Président et/ou collège	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, voy. le site Internet de la CPVP (http://www.privacycommission.be) et son Rapport annuel 2011. Voir aussi l'article 24 § 4 alinéas 3 et 4 : « La Commission est composée de telle façon qu'il existe en son sein un équilibre entre les différents groupes socio-économiques. Outre le président, la Commission comprend au moins, parmi ses membres effectifs et parmi ses membres suppléants, un juriste, un informaticien, une personne pouvant justifier d'une expérience professionnelle dans la gestion de données à caractère personnel relevant du secteur privé, et une personne pouvant justifier d'une expérience professionnelle dans la gestion de données à caractère personnel relevant du secteur public ».
Budget	5 684 000 EUR(2012)
Personnel	53 employés (1 Président — 1 Vice-président) - Secrétariat 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 ci-après) : 41 - Avis et recommandations d'initiative : 9 - Recommandations dans le cadre des déclarations de traitements ultérieurs : 9
Notifications	
Examens 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 vus adresser le nombre de demandes d'autorisations suivant : - Comité sectoriel Autorité fédérale : 46 (individuelles) et 40 (adhésions à des autorisations générales) - Comité sectoriel statistiques : 38 (individuelles) - Comité sectoriel du Registre national : 106 (individuelles) et 229 (adhésions à des autorisations générales - Comité sectoriel de la sécurité sociale et de la santé : voir le site de la banque-carrefour de la sécurité sociale
Demandes émanant des personnes concernées	Les statistiques de la Commission belge de la protection de la vie privée ne font pas de distinction selon que les demandes d'information proviennent de personnes concernées ou de responsables de traitement: - Information données par le Front Office : 1 892 dossiers « Questions — réponses » ouverts en 2012 (droit à l'image, principes de protection de la vie privée, économie/crédit à la consommation, vie privée sur le lieu de travail et autorités publiques. - La CPVP a en outre traité 2 896 demandes d'information ou de médiation (y compris des dossiers de contrôle) : Ces dossiers peuvent être répartis comme suit : 2 437 demandes d'informations émanant tant d'instances publiques et de responsables de traitement actuels ou futurs que de personnes concernées, 303 demandes de médiation et 156 dossiers de contrôle.
Plaintes émanant des personnes concernées	Voir Supra : 303 demandes de médiation : avant toute médiation ou communication d'information, la CPCP procède toujours à une analyse de recevabilité. Pour 149 dossiers, la demande de médiation s'est avérée irrecevable, souvent en raison d'un manque d'information de la personne concernée (144 dossiers). 198 demandes, soit 8,26 % ont été adressées erronément à la Commission de la protection de la vie privée, qui s'est toujours efforcée d'orienter le demandeur vers l'institution compétente. Dans

	près de 75 % des cas, la CPVP y est parvenue. Les thèmes les plus fréquemment abordés (information, médiation/plainte et contrôles) sont les suivants : - Traitement d'images dont, surtout, vidéosurveillance - Principes de la protection de la vie privée - Traitements de données par des autorités publiques - Pratiques commerciales (principalement marketing) - Vie privée et travail, crédit.
Conseils sollicités par le Parlement ou le gouvernement	La liste des avis émis par la Commission belge en 2011 est disponible sur son site Internet à l'adresse : http://www.privacycommission.be
Autres renseignements relatifs aux activités générales	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	156 contrôles. En 2012, la Commission de la protection de la vie privée a effectué des contrôles à 2 niveaux. Le 1er 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 3 types : 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 les dossiers dans lesquels elle constate des infractions au parquet.
Amendes	La CPVP ne dispose pas de compétence de sanction propre. Elle peut toutefois transmettre les dossiers dans lesquels elle constate des infractions au parquet.
DPD	
Chiffres relatifs aux DPD	La CPVP ne dispose pas de cette information.

BULGARIE

A. Résumé des activités et actualités

Organisation	Commission de protection des données à caractère personnel
Président et/ou collège	Commission composée d'une Présidente, Mme Veneta Shopova, et de 4 membres : M. Krassimir Dimitrov, M. Valentin Enev, Mme Mariya Mateva et M. Veselin Tselkov.
Budget	2 738 678 BGN, dont 2 573 917 BGN dépensés.
Personnel	Nombre de fonctionnaires employés : 78
Activités générales	
Décisions, avis, recommandations	En 2012 : 364 décisions, avis et instructions ont été émis au total, dont : - 271 plaintes - 77 avis sur l'application de la LPDP - 16 instructions contraignantes
Notifications	66 805 responsables du traitement des données à caractère personnel
Examens préalables	1 616
Demandes émanant des personnes concernées	247 demandes émanant de personnes physiques et d'entités juridiques et diverses demandes sur des thèmes d'actualité liés aux compétences de la CPDP.
Plaintes émanant des personnes concernées	531 plaintes — la plupart émanant des secteurs suivants : - Télécommunications : 274 - Services d'assurance et du travail : 33 - Banques et secteur bancaire : 32
Conseils sollicités par le Parlement ou le gouvernement	- Demande d'avis de l'Assemblée nationale sur la possibilité de faire une copie de la liste fournie avec les signatures collectées en vertu de la loi de participation directe des citoyens à l'autorité de l'État et aux autorités autonomes locales (ADPNSALS) pour interdire la recherche et l'exploitation en Bulgarie de gaz de schiste par fracturation hydraulique à soumettre aux membres du comité d'initiative et à introduire à l'Assemblée nationale. - Demande d'avis du Conseil des ministres sur la création d'un nouveau registre de données à caractère personnel et sur l'autorisation d'y avoir accès.

Autres renseignements relatifs aux activités générales	Concernant les transferts, la loi sur la protection des données à caractère personnel prévoit un système d'autorisation et, pendant la période prévue, huit demandes d'autorisation de transferts de données à caractère personnel vers des pays tiers ont été considérées. Concernant les règles d'entreprise contraignantes, la CPDP approuve l'autorité responsable et coordonne les documents sur l'approbation des règles d'entreprise en vertu de la procédure de reconnaissance mutuelle et, en 2012, 14 demandes d'approbation ont été déposées.
Activités d'inspection	
Contrôles, enquêtes	En 2012, le nombre total de contrôles réalisés a été de 1 718, dont : - *ex-ante* : 1 616 - en cours : 71 - *ex-post* : 32, la plupart dans les secteurs suivants : santé : 996 ; commerce et services : 109 ; éducation et formation : 106 ; tourisme : 58 ; services juridiques et de conseil : 54, etc.
Activités de sanction	
Sanctions	En 2012, l'activité de la CPDP en termes de sanctions imposées a été la suivante : - 58 actes de constatation de violations administratives - 52 amendes imposées
Amendes	En 2012, la CPDP a imposé des sanctions pour un montant de 323 350 BGN (environ 161 675 EUR).
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

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

En 2012, 16 instructions contraignantes ont été formulées, dont la plupart dans le domaine de l'administration publique, suivi du secteur financier, puis de la santé, les secteurs les moins concernés étant ceux du pouvoir judiciaire, de l'éducation et de la formation, des transports, du commerce et des 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 : 51 % des instructions ;

- l'absence des mesures nécessaires pour mettre à jour les informations soumises au registre des responsables du traitement de données à caractère personnel de la CPDP : 33 % ;
- l'interdiction de traitement de catégories de données à caractère personnel spécifiques : 13 % ;
- la violation de l'exigence de consentement éclairé de la personne avant le traitement de ses données à caractère personnel : 3 %.

Parmi les violations les plus courantes de la CPDP pour lesquelles des actes de constatation de violations administratives ont été formulés figuraient les suivantes :

- le non-respect de l'exigence de mise à jour des informations reçues dans les registres de données à caractère personnel fournis à la CPDP. La violation consiste à traiter un nouveau registre sans que le responsable du traitement ne le déclare à la CPDP ni ne l'entre dans le système ;
- l'absence d'instruction pour l'établissement de mesures techniques et organisationnelles visant à protéger les données de toute destruction accidentelle ou illégale, de toute perte fortuite, de tout accès illicite, de toute rectification ou diffusion et de toutes autres formes illégales de traitement ;
- le non-respect de l'obligation d'inscription auprès de la Commission de protection des données à caractère personnel ;
- la non-exécution des mesures techniques et organisationnelles nécessaires pour protéger les données de toute destruction accidentelle ou illégale, de toute perte fortuite, de tout accès illicite, de toute rectification ou diffusion et de toutes autres formes illégales de traitement.

2. En ce qui concerne la formulation d'avis sur des demandes et signaux (en dehors des cas cités dans le tableau) pour lesquels la CPDP a été approchée par les autorités publiques, les avis suivants sont également intéressants.

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

Parmi les demandes les plus souvent formulées figurent des demandes d'accès à la base de données démographiques nationale maintenue par les services d'état civil et administratifs (CRAS) de la direction générale et le ministère du Développement régional ou aux registres d'état civil.

Dans la plupart des cas, les responsables du traitement des données ont demandé à bénéficier d'un accès direct à la base de données démographiques nationale, motivé par l'existence d'un intérêt juridique.

La pratique de la CPDP vis-à-vis des demandes d'accès direct à la base de données démographiques nationale est qu'une distinction doit être faite entre la fourniture 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 CPDP estime qu'il n'y a aucun obstacle juridique à la soumission d'informations spécifiques, à savoir de données à caractère personnel, (et non un accès direct), conformément à la procédure définie sur le plan juridique par les services d'état civil et administratifs (CRAS) de la DG et le ministère du Développement régional afin d'exercer l'intérêt juridique, le cas échéant, des personnes demandant les informations.

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 2012, la CPDP s'est également prononcée sur des demandes d'avis de l'État et d'organismes locaux en lien avec l'accès à des informations publiques.

Les autorités publiques concernées ont notamment reçu des demandes de communication d'informations sur leurs rémunérations.

Après avoir considéré les questions soulevées, la CPDP a formulé un avis selon lequel les informations sur des postes spécifiques et leur rémunération répondent à la définition de « données à caractère personnel » du point de vue de l'identité de la catégorie économique, uniquement si la personne peut être positivement identifiée.

Le traitement de ces informations n'est admissible et légal que lorsque l'une des conditions d'admissibilité établies est respectée, comme l'existence d'un intérêt public ou le consentement explicite des personnes.

2.3. Concernant les demandes liées à la prévention des conflits d'intérêts dans le cadre de la désignation de fonctionnaires de haut niveau au sein de l'administration publique

En 2012, la Commission pour la protection des données a formulé un avis à la demande de la Commission pour la prévention et l'identification des conflits d'intérêts, sur l'admissibilité, en vertu de la LPDP, de la publication sur Internet (suite à une décision de la Commission pour la prévention des conflits d'intérêts) d'informations concernant :

- les titres de personnes exerçant une fonction publique, lorsque ces informations peuvent permettre l'identification de la personne ;
- le titre et le nom complet du lieu où cette fonction publique est exercée, lorsque ce lieu peut permettre l'identification de la personne.

Lors de l'examen de cette demande d'avis, la CPDP a tenu compte du fait que la Commission pour la prévention et l'identification des conflits d'intérêts est légalement tenue de publier ses décisions sur son site Internet en vertu de la loi sur la prévention et la constatation de conflits d'intérêts, de sorte que la publicité et la transparence du travail et des décisions de la Commission sont assurées et que l'autorité est également tenue de ne pas divulguer l'identité de la personne qui a envoyé le signal.

La CPDP a exprimé un avis selon lequel, lorsque des décisions de la Commission pour la prévention et l'identification des conflits d'intérêts sont publiées sur son site Internet, des mesures doivent être prises afin d'assurer l'impossibilité d'identifier les personnes physiques ayant envoyé un signal ou contre lesquelles un signal a été envoyé. À cet égard, outre l'initialisation des noms et adresses, les caractéristiques liées à l'identité physique, physiologique, génétique, psychique, psychologique, économique, culturelle, sociale ou autre d'une personne devraient être effacées. Conformément à l'objet de la loi sur la prévention et la constatation de conflits d'intérêts et à l'obligation des personnes exerçant une fonction publique de remplir leurs tâches dans l'intérêt du public, de manière honnête, juste, responsable et objective, et d'être responsables devant les citoyens et les autorités qui les ont choisies ou désignées, la CPDP a présumé que dans les décisions publiées sur le site Internet de la Commission, les données relatives à leur poste et/ou leur profession, ainsi que le lieu où celle-ci est exercée, pouvaient être publiés. Si la décision contient des données à caractère personnel de tierces personnes, celles-ci devront être rendues anonymes.

2.4. Avis de la CPDP sur la loi de participation directe des citoyens à l'autorité de l'État et aux autorités autonomes locales

Une autre demande d'avis intéressante a été formulée par l'Assemblée nationale sur la possibilité qu'une copie de liste d'abonnés soit communiquée, en vertu de la Loi de participation directe des citoyens à l'autorité de l'État et aux autorités autonomes locales, avec une demande d'interdiction de l'exploration et de la production de gaz de schiste par fracturation hydraulique en Bulgarie, à un membre du comité d'initiative qui en avait fait la demande à l'Assemblée nationale.

L'avis de la CPDP sur ce cas est que la communication d'une copie de liste d'abonnés à un membre du comité d'initiative représente une opération de « traitement de données à caractère personnel » par le biais de la communication de données conformément à la définition légale visée au paragraphe 1, alinéa 1, des dispositions supplémentaires de la LPDP. Des données à caractère personnel ont été collectées pour l'initiative civile nationale, et la liste d'abonnés a été communiquée à l'Assemblée nationale, dont la

copie était accompagnée du texte obligatoire indiquant que des données à caractère personnel ne sauraient servir à d'autres fins que celles de l'initiative citoyenne visant à faire interdire la recherche et l'exploitation du gaz de schiste par fracturation hydraulique en Bulgarie. La demande de communication d'une copie de la liste d'abonnés de l'initiative citoyenne nationale visant à faire interdire la recherche et l'exploitation du gaz de schiste par fracturation hydraulique en Bulgarie, préparée en vertu de la Loi de participation directe des citoyens à l'autorité de l'État et aux autorités autonomes locales, à un membre du comité d'initiative représentait une opération supplémentaire de traitement de données à caractère personnel à d'autres fins que celles pour lesquelles les données avaient été collectées et par des moyens incompatibles avec ces fins. C'est pourquoi une copie de la liste d'abonnés ne devrait pas être communiquée.

C. Autres informations importantes

1. La Commission de protection des données à caractère personnel a adopté une nouvelle ordonnance concernant le niveau minimal de mesures techniques et organisationnelles et de types admissibles 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 de types admissibles 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 et est entrée en vigueur trois jours après sa promulgation. Cette ordonnance abroge l'ordonnance n°1 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 de la protection des données. L'ordonnance définit les principaux objets de la protection des données à caractère personnel : confidentialité, intégrité et disponibilité. Elle introduit cinq types de protection des données à caractère personnel différents : protection physique, protection personnelle, protection documentaire, protection des systèmes d'information automatisés et/ou réseaux et protection cryptographique. L'ordonnance a par ailleurs introduit le principe du « besoin d'en connaître » dans le cadre du contrôle des accès.

Afin de déterminer le niveau adéquat de mesures techniques et organisationnelles et le type de protection admissible, les responsables du traitement sont tenus de réaliser régulièrement une évaluation de l'impact sur les données à caractère personnel traitées. L'évaluation de l'impact vise à déterminer les différents degrés de risques et les niveaux de protection correspondants. Chaque niveau de protection correspond à une combinaison précise des mesures organisationnelles et techniques que doivent mettre en œuvre les responsables du traitement.

Les nouvelles règles prévoient quatre niveaux d'impact, suivant le degré des effets indésirables pouvant découler du traitement non autorisé de données à caractère personnel : « extrêmement élevé », « élevé », « moyen » et « faible ».

Depuis que l'ordonnance est entrée en vigueur, la Commission a commencé les formations et consultations des responsables du traitement de données afin de les sensibiliser aux nouveaux problèmes concernant les données à caractère personnel.

L'ordonnance est disponible en anglais sur le site Internet de la CPDP.

En général, la Commission de protection des données à caractère personnel met l'accent sur la formation des responsables du traitement de données à caractère personnel conformément au plan de formation annuel adopté. En outre, les experts de la Commission de protection des données à caractère personnel sont invités par l'Institut de l'administration publique (le centre de formation national des fonctionnaires) à donner régulièrement des cours de formation sur la protection des données, et ce depuis octobre 2013.

2. Pratiques en vertu de la directive 2006/24/CE sur la conservation des données

La directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (directive « vie privée et communications électroniques ») a été transposée dans la législation bulgare via des amendements de la loi sur les communications électroniques en 2010. Après analyse des informations statistiques fournies en 2012 par les entreprises fournissant des réseaux et/ou services de communications électroniques, la Commission de protection des données à caractère personnel a analysé les problèmes et les tendances du processus de conservation des données relatives au trafic sur le plan national. La Commission a identifié les sujets de préoccupation suivants :

- Les fondement juridiques qui permettent de justifier d'une demande d'accès aux données relatives au trafic ne correspondent pas aux entités habilitées à soumettre ces demandes et aux différents organismes prévus par la LCE comme étant compétents pour demander des références, mais sont plus larges (le service d'intelligence national, par exemple, fait partie des autorités mandatées pour demander un accès alors qu'il n'a pas la compétence de divulguer et d'enquêter sur les infractions graves).
- La classification des demandes d'accès et la décision du tribunal empêchent les fournisseurs de services Internet n'ayant pas de registre d'informations classifiées de fournir des références.
- Les sociétés fournissant des réseaux et/ou services de communications électroniques ont exprimé leur inquiétude face à l'absence de contrôle des demandes d'accès de la part des forces de police judiciaire et au fait que certaines catégories de personnes obtiennent des références de données relatives au trafic de manière extrêmement facile. Le bureau du Procureur de la République de Bulgarie soutient l'approche selon laquelle, dans le cadre de procédures préliminaires, une demande d'accès devait être déposée par l'organisme en charge de l'enquête avec une autorisation écrite expresse du procureur responsable.
- Le nombre d'entreprises ayant respecté leur obligation légale de fournir des informations statistiques tend à diminuer (pour comparaison, en 2011, 33 entreprises avaient fourni des données statistiques et, en 2012, elles n'étaient plus que 22). Il semble néanmoins évident que les grandes entreprises de ce marché fournissent des informations précises qui, dans une large mesure, peuvent permettre de dégager des tendances et forment une base solide à des fins d'analyse statistique.
- Malgré la position de la CPDP selon laquelle l'exigence de la LCE en matière de communication d'informations sur les « cas où des données ont été fournies aux autorités compétentes » implique la communication de statistiques spécifiques et détaillées sur l'ensemble des cas distincts, les entreprises ne sont pas en mesure de communiquer ces informations et ne fournissent par conséquent que des données synthétiques sur le nombre total de cas de demandes d'accès.
- Le nombre de cas où les autorités compétentes ont demandé des données relatives au trafic a pratiquement doublé (pour comparaison, ce nombre s'élevait à 39 781 en 2011 et à 75 672 en 2012).
- Le nombre de cas où des données ont été communiquées aux autorités compétentes en vertu de la LCE a presque doublé (pour comparaison, en 2011, le nombre total de cas s'élevait à 38 861 et à 74 296 en 2012) ; le nombre de cas où la demande de données n'a reçu aucune réponse a également augmenté (pour comparaison, en 2011, ce nombre s'élevait à 920, et à 1 376 en 2012).
- Les informations statistiques reçues par la CPDP de la part d'entreprises sont synthétisées sur la base de différents critères et paramètres et ne sont pas totalement conformes aux types d'informations escomptés par la Commission européenne.

Pour répondre aux attentes de la Commission européenne et prendre des mesures en faveur de l'unification de la pratique au niveau national, la Commission de protection des données à caractère personnel a publié des instructions contraignantes à l'attention des entités responsables au titre de la LCE.

Ces instructions contraignantes réglementent l'ensemble des paramètres évoqués lors des réunions avec les institutions participant au processus de conservation des données.

Ces instructions spécifient les exigences relatives au contenu des registres maintenus par les autorités en vertu de l'article 250, paragraphe b, de la LCE, les tribunaux et les entreprises fournissant les réseaux et/ou services de communications électroniques accessibles au public, dans la mesure où il a été explicitement énoncé que ces exigences représentent le contenu minimum requis. Toute personne responsable peut également, en son entière discrétion, requérir la saisie d'informations supplémentaires dans les registres. Il est indiqué que l'enregistrement, le stockage et la destruction de documents liés aux demandes d'accès, aux autorisations données et aux refus, aux ordonnances d'accès et références, sont déterminés par le règlement intérieur de l'autorité en vertu de l'article 250, paragraphe b, alinéa 1, de la LCE, un tribunal ou une entreprise, pour travailler avec des documents ouverts et classifiés relevant des actes législatifs applicables. Les exigences de destruction des données stockées sont établies.

CHYPRE

A. Résumé des activités et actualités

Le bureau du commissaire a activement participé aux discussions sur le paquet de propositions pour la protection des données présenté par la Commission en janvier 2012. En février 2012, un protocole d'accord a été conclu entre le commissaire et le ministre de la Justice et de l'Ordre Public, établissant une procédure pour l'adoption de positions communes et désignant un délégué à la protection des données pour présider le DAPIX, le groupe de travail du Conseil qui devait discuter du paquet de propositions. En mars 2012, le bureau du commissaire, associé au ministère, a lancé une consultation publique sur ces propositions et a rencontré de nombreuses parties intéressées importantes avant et pendant la présidence chypriote. La présidence chypriote du DAPIX a avancé les discussions sur les propositions et identifié un certain nombre de questions horizontales pour lesquelles les délégations ont exprimé des inquiétudes communes, à savoir le grand nombre d'actes délégués et mis en œuvre incorporés aux propositions, le fardeau administratif pour les petites et moyennes entreprises et l'imprécision des règles / dérogations pour le secteur public, qui ont été discutées dans le cadre des réunions informelles des amis de la présidence. Le travail de la présidence chypriote est synthétisé au sein du rapport intermédiaire adopté par le Conseil des ministres JAI en décembre 2012.

Dans le cadre des activités de célébration de la Journée européenne de la protection des données, le bureau du commissaire a utilisé un budget de EUR 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 *Time for awakening, time for enlightenment* (il est temps de se réveiller et de comprendre). Le commissaire et ses délégués ont fait plusieurs apparitions à la télé et à la radio.

En 2012, la loi de base (Loi 138(I)/2001) a été amendée dans le but de mieux transposer les dispositions de la directive 95/46/CE conformément aux commentaires de la Commission dans le cadre d'un dialogue structuré et d'améliorer le bon fonctionnement du bureau du commissaire.

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 termes du contrat d'assurance et le nombre de documents (supplémentaires) parfois exigés de la plaignante, le commissaire a demandé à la société de justifier la raison pour laquelle elle n'avait pas, à un certain point, accepté ou rejeté la demande d'indemnisation, compte tenu du nombre proportionnel de documents, mais en avait prolongé l'examen en demandant des tests et documents supplémentaires, une pratique qui semble à première vue en violation du principe de proportionnalité. Le cas est encore en cours d'examen, en attente de la décision du commissaire.

Suite à l'examen d'une plainte déposée par des employés par le biais de leurs syndicats contre deux hôpitaux privés qui avaient récemment installé des systèmes de contrôle des horaires de travail faisant appel à des données biométriques (empreintes digitales) stockées uniquement 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. Les hôpitaux ont été appelés à cesser le traitement des données et à désinstaller les systèmes. Si un hôpital a respecté la décision, le deuxième l'a en revanche 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 : 307 570 EUR Budget exécuté : 265 609 EUR
Personnel	Agents administratifs : 7 Agents informaticiens : 2 Secrétaires : 6 Agents auxiliaires : 2
Activités générales	
Décisions, avis, recommandations	Avis : 47 Décisions : 5 Recommandations : 1
Notifications	260
Examens préalables	s. o.
Demandes émanant des personnes concernées	Par écrit ou par téléphone : s. o.
Plaintes émanant des personnes concernées	Autorisations de regroupement de systèmes de fichiers : 43 Autorisations de transmission vers des pays tiers : 46
Conseils sollicités par le Parlement ou le gouvernement	En 28 occasions, notre bureau a été invité aux réunions des comités parlementaires de la Chambre des représentants pour des conseils / consultations
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	Nombre d'audits : 1. Nombre de plaintes examinées : 233 sur 325
Activités de sanction	
Sanctions	Dans une décision du commissaire, la sanction administrative a été la cessation du traitement et la destruction des données à caractère personnel. Dans une autre décision, le Commissaire a adressé des recommandations au responsable du traitement.
Amendes	Dans 3 décisions, des amendes ont été imposées aux responsables du traitement pour un total de 3 500 EUR

DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

En 2011, le commissaire, conformément à l'article 23, paragraphe a), de la loi, a rapporté au chef de la police une possible infraction pénale commise par un site Internet journalistique n'ayant pas respecté la décision du commissaire de cesser le traitement et de détruire les données à caractère personnel de demandeurs d'asile qui avaient été publiées en violation du principe de proportionnalité, dans un article disponible sur le site pendant des semaines, et n'ayant pas payé les 3 000 EUR d'amende qui lui avaient été imposés. L'affaire a été portée devant le tribunal. Le défendant ayant informé le tribunal de son respect subséquent de la destruction des données et de la cessation de leur traitement, le tribunal a donné raison à la décision du commissaire et exigé du site qu'il paie l'amende en tant que dette civile.

DANEMARK

A. Résumé des activités et actualités

Organisation	Agence danoise de protection des données
Président et/ou collège	La gestion des affaires quotidiennes de la DPA est assurée par le Secrétariat, sous la conduite d'un Directeur. Les affaires particulièrement intéressantes (une quinzaine par an) sont soumises à la décision du Conseil. Le Conseil est présidé par un juge de la Cour suprême.
Budget	21,1 millions de DKK.
Personnel	Environ 35
Activités générales	
Décisions, avis, recommandations	s. o. (inclus dans les chiffres ci-dessous)
Notifications	2 031
Examens préalables	2 031
Demandes émanant des personnes concernées	2 062 Ce nombre couvre l'ensemble des demandes et plaintes déposées devant la DPA danoise
Plaintes émanant des personnes concernées	Voir ci-dessus
Conseils sollicités par le Parlement ou le gouvernement	444
Autres renseignements relatifs aux activités générales	26 affaires liées à la sécurité
Activités d'inspection	
Contrôles, enquêtes	58
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	Amendes imposées dans six cas.

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

B. Informations sur la jurisprudence

Retransmission de services religieux en direct

Une église de la ville de Ribe a contacté la DPA danoise avec une demande portant sur le respect de la loi danoise sur le traitement des données à caractère personnel et la retransmission d'un service religieux en direct. Cette retransmission avait pour objet de donner aux personnes ne pouvant être présentes pour diverses raisons une opportunité d'assister à la cérémonie. Un panneau à l'entrée de l'église décrivait clairement l'enregistrement vidéo ayant lieu dans l'église.

La DPA danoise a estimé que la congrégation était responsable du traitement des données à caractère personnel dans cette situation. Il revenait dès lors à la congrégation de peser les intérêts légitimes de la retransmission par rapport aux intérêts des personnes filmées.

À ces fins, il convient également de noter que le service religieux était ouvert au public et que les bénéficiaires de la retransmission étaient un groupe de personnes spécifique et limité, comme les personnes âgées d'une maison de retraite.

Dans son évaluation initiale, la DPA danoise a considéré que la loi danoise sur le traitement des données à caractère personnel n'interdit pas la retransmission de services religieux spécifiques, tant que les participants en sont clairement informés et que la transmission est contrôlée de manière à n'être retransmise qu'en certains lieux spécifiques. Dans certaines situations (un baptême, par exemple), le consentement écrit des participants reste nécessaire.

C. Autres informations importantes

Vidéosurveillance par des organismes de logement

En 2012, la DPA danoise a initié une série d'inspections spécialement consacrées à la vidéosurveillance dans les organismes de logement privés. Ce projet avait pour objet d'acquérir une expérience pratique dans ce domaine particulier et de sensibiliser au sujet de la protection des données par les sociétés privées et les personnes physiques. Les problèmes les plus courants portaient sur l'interférence de la conservation de données et de la prise de vues à grande échelle avec la sphère privée de certains appartements, même si un respect décent de la vie privée et de la protection des données a été observé de manière générale.

L'expérience accumulée dans le cadre de ce projet a permis la publication sur papier et en ligne d'un ensemble de lignes directrices exhaustives.

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.

BCR

Le Danemark a reçu de nombreuses demandes d'approbation de BCR, ce qui signifie que le pays devrait jouer le rôle d'autorité responsable en quelques occasions.

Un nombre croissant de sociétés danoises ont réalisé les opportunités du modèle de BCR, qui offrira une flexibilité accrue au transfert de données vers des pays tiers dès que les règles seront prêtes et auront été mises en œuvre. Avec la poursuite de cette évolution, la DPA danoise s'attend à ce que le nombre de demandes augmente à l'avenir.

En 2012, la DPA danoise a également été « co-lectrice » de BCR dans un processus de BCR impliquant l'ICO britannique en tant qu'autorité responsable.

ESPAGNE

A. Résumé des activités et actualités :

Plus encore que les années précédentes, 2012 a été marquée par une augmentation remarquable des activités de l'agence, notamment dans les domaines des activités de notification de traitement et d'inspection, avec des pourcentages de progression positifs de 15 % et 40 % respectivement. Tout au long de l'année 2012, nous avons travaillé à l'élaboration de mesures de simplification et de facilitation de l'exercice des droits des citoyens ainsi que de la conformité réglementaire. En ce sens, il convient de mentionner, notamment, le lancement de notre plateforme de services en ligne (https://sedeagpd.gob.es/sede-electronica-web/) ainsi que l'optimisation de tous les services d'information fournis via notre site Internet.

Concernant les activités d'inspection et l'exercice des pouvoirs de sanction, il convient de souligner que, bien que les chiffres sur les résolutions punitives restent stables, le nombre de résolutions donnant lieu à des avertissements écrits a considérablement augmenté (+ 34,2 % par rapport à 2011). L'emploi de cette possibilité, conjointement avec l'ensemble de critères qui peuvent désormais être utilisés pour graduer le montant des pénalités, permet de tempérer de manière substantielle la sévérité de la sanction en fonction de la gravité et des conséquences réelles de l'infraction.

L'agence maintient également ses efforts visant à assurer une meilleure protection des enfants. À cet égard, nous avons beaucoup travaillé tout au long de l'année à l'élaboration d'un site éducatif qui vise à fournir aux enfants et aux éducateurs des informations et des outils intéressants et qui devrait être lancé pour le dernier trimestre de 2013.

La mise en œuvre de la réforme de la directive « Vie privée et communications électroniques », transposée dans le droit national par un décret royal d'avril 2012, a également été une source importante d'activité. Depuis lors, l'agence a travaillé avec l'ensemble des parties intéressées aux niveaux national et international. Grâce à ces efforts, des documents de conseils et des outils liés à la mise en œuvre correcte des cookies sur la base des dispositions et des notifications de violations devraient être publiés en 2013.

Organisation	Agence espagnole de protection des données
Président et/ou collège	José Luis Rodríguez Álvarez
Budget	13 929 550 EUR
Personnel	159
Activités générales	
Décisions, avis, recommandations	11 907
Notifications	630 251
Examens préalables	s. o.
Demandes émanant des personnes concernées	111 933
Plaintes émanant des personnes	10 787

concernées	
Conseils sollicités par le Parlement ou le gouvernement	292
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	2 266
Activités de sanction	
Sanctions	896
Amendes	21 054 656,02 EUR
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Une première référence doit être faite à la décision de la Cour suprême de février 2012 en jugement des appels liés à l'arrêté royal 1720/2007 du 21 décembre, qui approuve le règlement mettant en œuvre la loi organique 15/1999 du 13 décembre sur la protection des données à caractère personnel. La décision déclare l'article 10.2.(b) du règlement invalide, en s'appuyant sur un jugement préliminaire de la Cour (jugement du 24.11.2011 dans les affaires C-468/10 et C-469/10 —ASNEF et FECEMD).

Les autres décisions pertinentes de la Cour suprême sont les suivantes :

Les informations relatives à une condamnation pour abus sexuel ne peuvent être considérées comme des données relatives à la vie sexuelle au sens de l'article 8 de la directive 95/46 ;

Une clause de consentement permettant l'envoi d'offres commerciales d'un groupe de sociétés peut être considérée comme suffisante pour envoyer des offres d'emplois de la part des mêmes entités ;

La charge de la preuve liée au respect du devoir d'information incombe au responsable du traitement ;

Les appareils de vidéosurveillance ne peuvent servir à contrôler le respect des règles sur le temps de travail que si les personnes concernées ont été dûment informées par avance de cette possibilité ;

Le secret professionnel est enfreint lorsque des données de santé (dans ce cas, la liste des patients recevant un traitement à la méthadone) sont publiées sur le panneau d'affichage d'un centre de soins. Il en va de même lorsque des données sont rendues accessibles via un système de partage de fichiers en pair-à-pair ;

Toujours en ce qui concerne le secret professionnel, la publication dans un journal officiel d'une condamnation pour une infraction pénale commise par un employé public est considérée comme une violation du secret professionnel ;

La simple existence d'une plainte n'oblige en aucun cas l'autorité de contrôle à initier une procédure d'infraction.

La Haute Cour nationale (Audiencia Nacional) a également été assez active en 2012 dans le domaine de la protection des données. Ses décisions les plus notables sont les suivantes :

- Les photos d'enfants ne peuvent être téléchargées et publiées sur les sites de réseaux sociaux qu'avec le consentement préalable des parents ou des tuteurs légaux. De même, il est obligatoire de mettre en place des mécanismes favorisant la vérification de l'âge et d'obtenir le consentement parental lorsqu'un responsable du traitement a l'intention de traiter les données d'un enfant dans le cadre de campagnes marketing sur Internet.
- Concernant la décision de la Cour Suprême sur l'application de l'intérêt légitime comme base légale du traitement de données, plusieurs décisions de la Haute Cour nationale s'appliquent dont, notamment, les suivantes :
    - L'intérêt légitime d'un journal a été considéré comme prévalant en cas de publication de détails sur des avis de sanction liés à des personnes exerçant une fonction publique. Il en va de même pour la publication de détails permettant d'identifier des candidats à des postes de la fonction publique ;
    - L'intérêt légitime d'un syndicat a également été considéré comme prévalant pour le traitement des données du personnel en interne et à des fins ayant un rapport direct avec la représentation des travailleurs ;
    - Il en est de même pour l'utilisation des coordonnées des membres d'une chambre professionnelle par d'autres membres au cours d'un processus électoral interne ;
    - D'un autre côté, l'intérêt de compiler une base de données contenant les données de trente-sept millions de personnes n'a pas été considéré comme prévalant alors que l'intérêt allégué en était la simple intention de commercialiser la base de données.
- Il a été considéré comme licite d'ajouter des images comme preuves obtenues par un enquêteur privé au dossier d'une affaire judiciaire lorsque ces images ont été acceptées par le juge au cours des procédures. Au contraire, il a été considéré comme illicite d'inclure des photos d'une personne à la vitrine d'un photographe sans le consentement de cette personne.
- L'impression sur une enveloppe de la phrase « patient atteint de la maladie cœliaque » lors de l'envoi de publicités pour des produits a été considérée comme constituant un cas de traitement de données de santé. Toujours dans le domaine des données sensibles, créer un faux profil prétendant être une tierce personne sur un réseau social s'adressant principalement à la communauté homosexuelle a été considéré comme constituant un traitement de données sur la vie sexuelle.

C. Autres informations importantes

L'affaire Google a aussi joué un rôle important tout au long de l'année en raison des questions en cause et de l'implication de la Cour européenne de justice à la demande de la Haute Cour nationale espagnole. L'affaire en tant que telle a commencé par la demande d'un citoyen à exercer son droit d'opposition au traitement fait par un journal (un avis publié plusieurs années auparavant) et lié à des informations qu'il considérait non seulement comme désuètes mais aussi sans objet malgré le fait qu'elles pouvaient l'affecter dans sa vie actuelle dans la mesure où il était facile de les trouver sur Internet grâce aux moteurs de recherche.

Le journal a refusé la suppression des données en arguant qu'elles avaient été publiées en raison d'une obligation légale découlant d'une ordonnance émanant d'une autorité compétente.

Par la suite, le citoyen a exercé son droit de recours à l'encontre de Google et demandé la suppression des liens menant à l'article sur le site web du journal. L'entité à laquelle il s'est adressé était alors Google Spain, SL. Cette demande a également été rejetée par l'entité.

Le citoyen a fini par déposer une plainte devant la DPA espagnole dans le but de s'assurer que ses droits seraient dûment exercés. Il s'est alors adressé aux deux entités Google Inc. et Google Spain, SL.

En réponse à cette plainte, la DPA espagnole a émis une décision demandant à Google Inc. et Google Spain de se plier à l'exigence du citoyen. Aucune mesure n'a été prise à l'encontre du journal.

Les deux entités ont alors fait appel de cette décision devant la Haute Cour nationale. La Cour a pris cette affaire en compte conjointement avec plusieurs décisions préalables prises dans des circonstances similaires. Compte tenu de l'augmentation du nombre de requêtes et de la nature des problèmes en cause, la Cour a décidé d'organiser une audience publique avec les deux parties afin qu'elles y présentent leurs points de vue. La Cour a également décidé de s'adresser à la Cour de justice de l'UE pour un jugement préliminaire.

Les deux principaux problèmes en jeu sont les suivants :

a) D'une part, l'applicabilité de la directive 95/46 aux 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 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) 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 porte sur la nature réelle des responsabilités légales de l'entité offrant le service... directe, complète ou simplement subsidiaire, du responsable du traitement responsable du site web où les informations ont été traitées à l'origine. Compte tenu de ce qui précède, et conformément aux critères de la Cour, il serait possible de faire une interprétation s'adressant directement au responsable du traitement du moteur de recherche afin d'éviter l'indexation des informations affectées.

Une décision finale est attendue pour le dernier trimestre 2013.

ESTONIE

A : Résumé des activités et actualités :

L'Inspection publique de protection des données a pour principale mission de s'assurer que :

- le droit à la vie privée d'une personne est respecté lorsque des données à caractère personnel sont utilisées ;
- les informations publiques sont accessibles.

L'Inspection est par conséquent le régulateur indépendant et l'agence en charge de l'application de la loi sur la protection des données à caractère personnel et de la loi sur les informations publiques.

Le législateur a également assigné différentes tâches supplémentaires à l'Inspection. Des missions liées à la législation internationale nous ont également été confiées ([6]).

En tant que protecteur des droits fondamentaux liés à l'information, l'Inspection joue le rôle de commissaire indépendant qui résout les plaintes et enquête sur les violations de sa propre initiative. Le nombre de demandes et de cas de supervision s'est stabilisé ces dernières années :

	2012	2011	2010
Demandes d'explication / d'information et mémorandums reçus	877	940	893
Appels à l'assistance téléphonique	1202	816	1061
Procédures de supervision initiées[2]	595	481	588
Procédures diverses (complétées)	43	34	35

L'utilisation de données à caractère personnel peut être considérée comme un sujet courant pour les demandes et procédures :

a) dans les relations de travail (contrôle des employés, pertinence d'un consentement ou d'un contrat pour le traitement de données, poursuite de l'utilisation d'une adresse électronique au nom d'un ancien employé) ;

b) concernant la divulgation d'informations sur l'endettement (principalement, la divulgation sans le filtre de l'intérêt légitime, la divulgation des membres de la direction d'entités endettées) ;

c) sur les réseaux sociaux et en ligne (en termes simple, ceci peut être décrit comme la demande d'une personne de faire disparaître son nom de moteurs de recherche sur Internet, la plupart du temps dans le cadre des réseaux sociaux) ;

([6]) Le législateur a assigné à l'Inspection des tâches supplémentaires dans le cadre de la **loi sur les communications électroniques** (supervision du marketing direct électronique même s'il ne concerne pas les données à caractère personnel, traitement des notifications de violations des entreprises de communication tout en permettant de ne pas informer les personnes concernées, éléments distincts des délits mineurs), la **loi sur les statistiques officielles** (participation au travail du Conseil des statistiques, éléments distincts des délits mineurs), la **loi sur la mise en œuvre du règlement (UE) n°211/2011 du Parlement européen et du Conseil relatif à l'initiative citoyenne** (certifiant la conformité des systèmes en ligne pour la collecte de déclarations de soutien), la **loi sur les signatures numériques** (suspension de l'utilisation de certificats en cas de suspicion), la **loi sur la recherche sur le génome humain** (approbation de la méthode de génération de codes pour les données), la **loi sur le registre de la population** (exprimant un avis sur la désignation du responsable autorisé du traitement du registre, approuvant le contrat de maintien du registre, autorisant les contrats de traitement exceptionnel de données), la **loi sur le registre environnemental** (exprimant un avis sur la désignation du responsable autorisé du traitement du registre, autorisant l'utilisation croisée de données à caractère personnel). Certaines tâches découlent **directement de la législation internationale**, notamment en ce qui concerne la participation à la supervision conjointe des systèmes d'information transfrontaliers (le système d'information Schengen, le système d'information Europol, le système européen d'information sur les visas, le système d'information douanier et le registre Eurodac d'empreintes digitales).

d) concernant le marketing direct électronique (publicités non sollicitées envoyées par courriel et message texte).

L'utilisation de caméras pour surveiller des personnes ainsi que la publication d'enregistrements sur les réseaux sociaux, au sein des sociétés et des établissements d'enseignement sont des problèmes croissants.

Sur le plan juridique, l'objet des questions et des litiges porte en général sur la base légale du traitement des données (si le consentement de la personne pour le traitement des données a été obtenu ou non, si un contrat ou un acte juridique aurait pu constituer la base légale du traitement sans consentement ou non).

Un nombre moins important de cas concerne les informations publiques (10 % de demandes d'explication, 18 % d'appels passés aux lignes d'information et un quart de plaintes et contestations).

Restreindre l'accès reste le sujet le plus courant dans le domaine des informations publiques : ces restrictions peuvent être excessives autant qu'inadéquates (accès aux documents représentant une violation de la vie privée via des registres de documents en ligne).

Toutefois, les litiges juridiques les plus complexes découlent de la question de savoir si une personne de droit privé peut être quelqu'un qui remplit une mission de service public et possède par conséquent également des informations publiques.

L'utilisation abusive du registre de la population est la raison la plus courante de procédures contraventionnelles (30 procédures complétées sur 43). L'utilisation abusive des bases de données de la police a diminué (4 procédures contraventionnelles).

Notre principal objectif est de mettre un terme aux violations, non de les punir. La majorité des violations prennent fin immédiatement avec la supervision ou lorsqu'une recommandation / proposition est reçue. En 2012, nous avons émis des préceptes dans 48 cas ([7]). Nous avons imposé des amendes coercitives et contraventionnelles dans 39 cas.

Organisation	Inspection estonienne de la protection des données
Président et/ou collège	Directeur général
Budget	595 403 EUR
Personnel	18
Activités générales	
Décisions, avis, recommandations	582
Notifications	608 enregistrements de traitements de données à caractère personnel sensibles
Examens préalables	23
Demandes émanant des	877

([7]) Ce chiffre n'inclut pas les préceptes standard permettant de garantir l'obligation d'enregistrer les responsables du traitement de données à caractère personnel sensibles (ces cas étaient au nombre de 130 en 2012).

personnes concernées	
Plaintes émanant des personnes concernées	404
Conseils sollicités par le Parlement ou le gouvernement	21
Autres renseignements relatifs aux activités générales – avis sur des systèmes d'information du secteur public	84
Activités d'inspection	
Contrôles, enquêtes	457
Activités de sanction	
Sanctions	40 cas
Amendes	5 918 EUR
DPD	
Chiffres relatifs aux DPD	137

B. Informations sur la jurisprudence

Le nombre de procédures concernant l'utilisation abusive de données de santé a augmenté en 2012. La raison en est simple : nous avons établi une coopération avec le Conseil de la santé et la Fondation e-Santé. Nous échangeons des informations sur de possibles violations. Nous avons réalisé deux audits dans le secteur de la santé et conclu que l'organisation de la protection des données à caractère personnel au sein de l'Agence nationale des médicaments et du Fonds d'assurance maladie respecte les exigences.

Dans le domaine de la supervision de la maintenance des bases de données, nous avons également réalisé des audits de la protection des données à caractère personnel auprès du gouvernement local de Viljandi, des services de secours et des autorités municipales de Narva, la supervision de ces deux dernières entités se poursuivant en raison de l'identification d'omissions.

Dans l'intérêt du traitement légitime des données, nous avons contrôlé les entrées du registre des auto-restrictions des joueurs (administration fiscale et douanière, les omissions ont été éliminées et la supervision a cessé), du logiciel de paie des agences publiques (ministère des finances, l'inspection de suivi devait se poursuivre en 2013) et de la base de données du Fonds estonien d'assurance automobile (l'inspection de suivi devait se poursuivre en 2013).

La concertation qui s'appuie sur les descriptions détaillées chargées dans le système d'administration du système d'information public contribue également à identifier les problèmes dans le domaine de la maintenance des bases de données. L'Inspection fait partie des agences de coordination qui surveillent le respect des exigences de protection des données à caractère personnel et d'information publique. Le nombre de procédures de concertation était de 84 en 2012 (dont 16 refus) et de 81 en 2011.

Le suivi comparatif de la divulgation des informations sur l'endettement des personnes physiques en novembre 2012 couvrait les sites Internet de 66 sociétés de recouvrement. 12 d'entre elles avaient divulgué les noms ainsi que, souvent, les dates de naissance ou codes d'identification personnels de personnes physiques sur des sites Internet publics. Sept de ces sociétés ont volontairement mis fin à ces violations, et cinq l'ont fait après que nous leur ayons adressé des préceptes.

C. Autres informations importantes

L'examen des demandes d'explication et des plaintes est une réaction destinée aux personnes et aux questions individuelles. Pour résumer, il s'agit de s'occuper des arbres plutôt que de la forêt.

Nous devons employer le peu de ressources dont nous disposons après avoir réagi aux problèmes de la manière la plus efficace : pour la prévention des problèmes, la communication d'informations, la préparation de lignes directrices, le soutien à d'importantes initiatives et le développement de la coopération.

Préparer l'ouverture du marché de l'électricité est un exemple de prévention : l'Inspection a participé au groupe de pilotage de l'entrepôt de données du marché de l'électricité pendant un an en tant que conseiller sur les problèmes liés à la protection de la vie privée des clients. Un seul véritable incident s'est produit par la suite dans ce domaine ([8]).

Notre première priorité en matière de protection des données à caractère personnel en 2012 a été la protection de la vie privée des mineurs. Nous avons consacré notre conférence annuelle (qui s'est tenue le 27 janvier) à ce sujet. Les lignes directrices du Chancelier de la justice sur les informations relatives aux enfants ayant besoin d'assistance ont également été présentées lors de la conférence. Nous avons rejoint le projet de coopération *Targalt Internetis* (Soyez intelligents en ligne !) organisé par l'union estonienne pour le bien-être de l'enfant (nous ne pourrions pas toucher un public aussi large si nous agissions seuls). Nous avons ciblé le jeu en ligne *Päästa Liisa ID* (Sauve l'identité de Liisa) destiné aux adolescents. Nous avons continué de donner des informations sur le compte utilisateur ouvert pour le jeu sur les réseaux sociaux. Nous avons parlé aux enseignants en sciences sociales lors du séminaire organisé par l'association estonienne du traité de l'Atlantique (le 26 octobre).

La coopération avec l'inspection du travail en 2012 s'inscrit dans la continuité des lignes directrices de 2011 sur la protection des données à caractère personnel dans le cadre des relations de travail. Nous avons participé aux quatre séries de conférences régionales organisées par l'inspection du travail et expliqué le sujet des données à caractère personnel des employés aux employeurs, aux spécialistes des ressources humaines et aux syndicats. L'inspection du travail a également publié nos lignes directrices en estonien et en russe. Nous remercions vivement nos collègues de l'inspection du travail pour leur importante coopération.

L'Estonie est devenue membre de la Convention de Schengen en 2007. L'abolition des contrôles aux frontières intérieures a été compensée par un échange d'informations entre les autorités policières des États membres via le système d'information Schengen et le système d'information sur les visas. Le risque que les systèmes d'information puissent faire l'objet d'une utilisation abusive est géré par des règles de protection des données strictes. Une fois tous les cinq ans, les États membres s'évaluent les uns les autres afin de vérifier le respect des exigences de Schengen par les autorités respectives dans leurs activités. Des comités d'évaluation composés de représentants des autorités de protection des données contrôlent l'adhésion aux règles de protection des données. Cette activité inclut l'évaluation du travail quotidien de supervision de la police, des gardes-frontières et des services consulaires dans le domaine de la protection des données ainsi que des capacités générales et de l'indépendance des autorités de protection des données.

([8]) L'un des fournisseurs d'électricité, 220 Energia OÜ, a rendu possible l'accès aux données des consommateurs sur la base de leurs codes d'identification personnels. Une tentative d'utilisation abusive de cet accès a été immédiatement détectée et la possibilité d'accès a été restreinte à la présentation de cartes d'identité.

L'Inspection a participé à l'évaluation de six autorités étrangères en 2011 et 2012. Les États baltes ont été évalués en octobre 2012. L'Estonie avait besoin d'une évaluation de suivi dans le domaine de la protection des données en 2007 mais, cette fois, l'évaluation s'est déroulée sans qu'aucune observation ne soit nécessaire.

Le comité d'évaluation a jugé exemplaires nos informations en ligne sur Schengen (informations approfondies et harmonisées dans trois langues sur les sites Internet de l'Inspection et des autorités associées), la coopération régulière entre les autorités estoniennes et les activités des autorités baltes de protection des données.

Nous souhaiterions souligner la contribution de nos collègues de l'Office de police et des garde-frontières, du ministère de l'Intérieur, du ministère des Affaires étrangères et du Centre des technologies de l'information et du développement du ministère de l'Intérieur dans l'obtention des résultats positifs de cette évaluation.

Des lignes directrices détaillées destinées aux envoyeurs et aux destinataires de publicités en ligne ont été complétées le 22 février 2012 dans le domaine du marketing direct électronique. La version préliminaire de ces lignes directrices a été évoquée par le comité consultatif public de l'Inspection ainsi qu'avec les organisations commerciales et le Conseil de la protection des consommateurs. Les lignes directrices ont été présentées dans le journal d'affaires *Äripäev* le 15 mars 2012. Nous nous référons également en permanence à ces lignes directrices dans le cadre de nos procédures et de nos correspondances.

Les autorisations de recherche scientifique ont constitué notre principale activité dans le domaine de la recherche et des statistiques. En 2012, nous avons émis 13 autorisations et refusé d'en émettre à trois reprises. Nous avons également réalisé des inspections aléatoires de suivi de la sécurité des données au sein d'institutions de recherche auxquelles nous avions accordé des autorisations. En 2012, nous avons inspecté l'Institut de la démographie de l'Université de Tallinn, où aucune omission n'a été relevée.

Nous avons aussi observé le recensement de la population et du logement qui s'est tenu au premier trimestre 2012. Nos collègues de l'administration du système d'information estonien nous ont aidés et conseillés. Statistics Estonia a rapidement éliminé les petites omissions identifiées sur le recensement en ligne, et aucun problème majeur n'a été observé. Dans l'état actuel de nos connaissances, la participation au recensement estonien en ligne a battu un record mondial : 62 % de l'ensemble des personnes concernées.

Dans le cadre de la coopération internationale, l'Inspection a participé aux activités de nombreux groupes de travail.

La coopération entre les inspections de la protection des données baltes a été un succès d'un point de vue pratique : nos collègues lituaniens ont rejoint le partenariat des autorités estoniennes et lettones en 2012. Nous avons réalisé, dans l'ensemble des hôtels de l'enseigne Radisson Blue, un audit conjoint sur le traitement des données à caractère personnel des clients et des membres du personnel.

Nous poursuivrons les activités conjointes de supervision en 2013, et notre attention se portera alors sur le secteur du jeu.

Le plan de réforme de la protection des données de l'Union européenne a été le sujet international le plus important. L'avis des autorités européennes de protection des données sur le plan de réforme, adopté le 23 mars 2012, était globalement positif, mais contenait également un certain nombre d'observations et de critiques. Cet avis n'était pas unanime, de nombreuses autorités de protection des données ne le soutenant pas pour diverses raisons.

La mise à jour de documents internationaux plus généraux a également été discutée dans le cadre du plan de réforme de la protection des données de l'Union européenne. L'Inspection participe au comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe. Les négociations des experts autour de l'amendement de la Convention de 1981 ont pris fin en 2012.

Nous représentons également l'Estonie au sein du groupe de travail sur la vie privée et la protection des données de l'Organisation de coopération et de développement économiques (OCDE) avec le ministère des Affaires économiques et des communications. Le groupe de travail discute des amendements à apporter au document central sur la vie privée de l'OCDE (Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel). Les discussions sont toujours en cours.

FINLANDE

A. Résumé des activités et actualités

La proposition de la Commission comprend, notamment, une proposition de mécanisme de contrôle de la cohérence, c'est-à-dire, d'instrument juridique destiné (comme la réforme dans son ensemble) à mieux harmoniser la protection des données et à créer un véritable marché unique du numérique en Europe. Dans le cadre de ces questions de protection transfrontalière des données, la prise de décision aurait lieu au sein d'un nouveau comité européen de la protection des données qui reste à établir. Toutefois, puisque ces questions transfrontalières semblent pour la plupart déjà d'actualité sur un plan « local » pour les pays nordiques, nous avons déjà mis en pratique l'utilisation de cet instrument avec nos collègues nordiques.

En novembre 2011, la Finlande a dû faire face à un barrage de pirates informatiques. Qu'avons-nous appris de ces violations de la sécurité ? Nous avons essayé de répondre à cette question pendant l'année considérée en réalisant une étude approfondie des parties qui avaient été attaquées par les pirates informatiques. Nous avons cherché à identifier quelles sortes de problèmes les violations de sécurité avaient causées et quels types de mesures les organisations avaient pris pour remédier à cette situation. Les résultats finaux de cette étude étaient plutôt sombres : la plupart des personnes interrogées ont déclaré s'être retirées du marché numérique suite à ces violations de sécurité. L'une des réponses les plus courantes était l'absence de réaction de la part du responsable du traitement !

Lors de la préparation de l'étude susmentionnée, nous avons organisé un grand atelier sur la sécurité des données à l'occasion du 25e anniversaire de notre bureau. Dans le cadre de cet atelier, les invités (sélectionnés parmi les personnes les plus compétentes du secteur) ont dû répondre à deux questions : est-il nécessaire d'améliorer la sécurité des données en Finlande et, si oui, les compétences pour le faire sont-elles disponibles ? Malheureusement, la réponse à la première question fut affirmative et la réponse à la seconde négative. Peut-être que le guide sur les comptes de données que nous avons publié aidera les organisations dans l'utilisation de leurs capacités en comptabilité moderne.

Outre l'atelier susmentionné, des ateliers sur l'édition d'annuaires téléphoniques, les réseaux sociaux (afin de déterminer l'existence de « zones grises » que les autorités ne peuvent régir sur les réseaux sociaux), le contrôle opérationnel volontaire et la protection des données pour les entrepreneurs ont été organisés au cours de l'année de référence. Cette année anniversaire a culminé à l'occasion d'un séminaire intitulé KnowRight2012 qui s'est tenu en Finlande, et dont nous étions l'un des organisateurs.

Alors que le Conseil de l'Europe rédigeait une recommandation sur le profilage, nous publiions une étude sectorielle sur les systèmes de fidélité des clients mis en œuvre en début d'année ([9]). Nous nous sommes aperçus que la qualité juridique des systèmes de fidélité des clients était relativement variable. Certaines des personnes interrogées n'ont pas su dire la raison pour laquelle elles utilisaient un système de fidélité des clients.

Organisation	Bureau du Médiateur chargé de la protection des données
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 1 737 000 EUR.

([9]) L'étude sectorielle est un outil que nous avons développé. Son objectif est le déploiement d'activités d'inspection aussi efficaces que possible, à l'aide de moyens technologiques.

Personnel	L'effectif total comprend 20 personnes.
Activités générales	
Décisions, avis, recommandations	2 946
Notifications	427
Examens préalables	Voir notifications
Demandes émanant des personnes concernées	986
Plaintes émanant des personnes concernées	(Accès et rectifications) 180
Conseils sollicités par le Parlement ou le gouvernement	122
Autres renseignements relatifs aux activités générales	Collaboration avec les responsables du traitement des données dans les secteurs suivants : éducation, soins de santé, affaires sociales, télécommunications, emploi et économie, marketing
Activités d'inspection	
Contrôles, enquêtes	102
Activités de sanction	97
Sanctions	s. o.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	> 1 000

B. Informations sur la jurisprudence

À la demande du médiateur chargé de la protection des données, le comité de la protection des données a commenté la solidité du système d'identification requis dans certains systèmes de réservation. Il s'agissait en l'occurrence de juger de la qualité juridique du service en ligne d'une chaîne de magasins d'optique où il est notamment possible de prendre rendez-vous en entrant son nom et son numéro de sécurité sociale. Le comité a manifesté son accord avec le point de vue du médiateur selon lequel le système en question n'était pas suffisamment sûr et les numéros de sécurité sociale servaient à distinguer les personnes au sein de la base de données. Le responsable du traitement en question a entrepris de remédier à ces faiblesses de son système.

Sur demande du médiateur chargé de la protection des données, le comité de la protection des données a étudié la vidéosurveillance de cages d'escaliers de bâtiments résidentiels, considérant qu'il s'agissait d'une question de principe importante. Il était notamment question du rapport entre la loi sur les données à

caractère personnel et le Code pénal finlandais. Le comité a estimé que la vidéosurveillance était possible également dans ce type d'immeuble en se basant sur les stipulations de la loi sur les données à caractère personnel.

C. Autres informations importantes

En partie en raison de l'absence d'exhaustivité de la praxis juridique, le ministère des Transports et des communications a commandé une étude sur le statut législatif des successions numériques au professeur en droit successoral Urpo Kangas de l'Université d'Helsinki. L'une des conclusions du rapport était que des règlements juridiques plus spécifiques devraient être créés.

Le médiateur chargé de la protection des données a aidé l'autorité de protection des consommateurs à déterminer des politiques sur la nature juridique des services basés sur des informations géographiques et financés par la publicité. Dans ce cas, la principale question portait sur le lien entre conditions contractuelles et consentement.

De nombreux développements intéressants

Un projet de législation a été poursuivi au cours de l'année de référence, avec la compilation d'un « code de la société de l'information ». Notre bureau a également participé au travail du groupe de pilotage et des sous-groupes spécifiques, dans toute la mesure du possible. À mon avis, les parties qui opèrent dans le domaine de l'économie numérique et de la production de services ont des difficultés à identifier la législation permettant de guider leurs opérations et ce, principalement en raison de la nature fragmentée de la législation ([10]). C'est l'une des raisons pour lesquelles les parties qui déploient leurs activités dans le secteur peuvent hésiter et douter, ce qui peut au final s'avérer une entrave au développement.

Une réforme importante qui n'a bénéficié que d'une attention limitée portait sur la mise en œuvre du numéro d'identification fiscale des employés. En Finlande, chaque personne reçoit un numéro de sécurité sociale (HETU) qui est entré dans le registre de la population, et un identifiant électronique destiné aux interactions avec les autorités (SATU). L'administration fiscale a par ailleurs mis en œuvre un numéro fiscal pour l'ensemble des employés dans une tentative d'enrayer le marché gris. À ce sujet pour le moins, l'administration publique semble gérer les risques liés à la gestion des identités. D'un autre côté, le développement de services mobiles basé sur le SATU a connu un départ relativement lent.

Un autre progrès de l'administration publique est le développement réglementé par la loi sur l'administration des données publiques, entrée en vigueur en 2011 : la centralisation du contrôle de l'utilisation des technologies de l'information a été renforcée aux décideurs des entreprises publiques. L'une des propositions avancées cette année concernait l'établissement d'une société de services informatiques détenue par l'État. L'audit national basé sur le décret sur la sécurité des données semble avoir pris un bon départ.

Bilan sur les données

Le 24 avril 2012, le bureau du médiateur chargé de la protection des données a publié un guide sur la préparation du bilan des données. Le bilan des données est un rapport de gestion des connaissances basé sur un examen interne qui vise à aider les organisations à évaluer leurs pratiques en matière de traitement des données. Il peut également servir à rendre compte des principaux problèmes de traitement des données aux parties intéressées d'une organisation. Le bilan des données se veut un outil dynamique qui favorise l'efficacité, l'impact et la compétitivité d'une organisation.

([10]) Citons par exemple un projet de loi du Gouvernement sur la réglementation de l'utilisation de données biométriques dans le cadre de la loi sur la radioprotection étudiée par le Parlement. Aucune loi finlandaise ne traite spécifiquement des données biométriques.

S'il est vrai que le bilan des données peut suppléer les rapports légaux basés sur les déclarations financières et les examens annuels, il n'a pas pour objet d'alourdir de manière indue le fardeau administratif d'une organisation. Le bilan des données respecte en outre le principe de responsabilité en vertu duquel une organisation doit démontrer par elle-même son respect de la législation et des bonnes pratiques en matière de traitement des données et de gestion des informations. À l'avenir, la législation relative à la protection des données pourra requérir l'introduction de pratiques conformes au principe de responsabilité.

Ce guide n'a pas pour objet de présenter une formule ou une liste d'informations exhaustive à inclure au bilan des données. Son contenu peut varier en fonction du secteur où évolue l'organisation et de la nature de ses opérations. C'est pourquoi il est recommandé d'introduire le bilan des données dans la mesure où celui-ci devrait avoir un impact positif sur les opérations de l'organisation.

Le bureau du médiateur chargé de la protection des données a participé au contrôle des problèmes susmentionnés et au contrôle de la recherche scientifique, à la supervision de la collecte d'échantillons ADN, aux problèmes liés aux systèmes de transport intelligent et aux péages routiers, à la communication sur les menaces de fuites de données des smartphones, à la réforme de la loi sur le traitement des données à caractère personnel par la police, au travail du comité des droits de l'homme et à de nombreux autres projets. Outre l'intensité de ces tâches quotidiennes (pour lesquelles de plus amples informations sont données dans d'autres sections de ce rapport annuel), nous devons adopter un point de vue plus large pour aborder certains problèmes. Une partie de ce point de vue plus large s'explique par la vaste coopération actuelle entre pays européens et nordiques ([11]) et une autre par notre participation à NETSO, un projet financé par l'académie de Finlande et dirigé par le professeur Ahti Saarenpää, qui étudie de manière horizontale le développement de la société d'information.

([11]) Dans le cadre de la coopération des pays nordiques, nous avons mis en œuvre un vaste examen de Facebook avec nos collègues norvégiens. Cet examen a commencé en 2011.

FRANCE

A. Résumé des activités et actualités

L'année 2012 a été marquée par une activité en hausse et les nombreuses initiatives prises par la CNIL pour accompagner les acteurs, qu'ils soient publics ou privés, dans leur démarche de conformité.

Le projet de règlement européen : un enjeu majeur pour la France

La Commission européenne a proposé le 25 janvier 2012 une réforme de la directive de 1995 sur la protection des données personnelles, en deux volets : une proposition de règlement définissant un cadre général et une proposition de directive relative aux données traitées à des fins de police et de justice.

Si la CNIL souscrit aux objectifs poursuivis par cette réforme (renforcement du consentement des personnes, reconnaissance d'un droit à la « portabilité » des données, simplification des démarches administratives pour les entreprises), elle a toutefois des interrogations quant à l'effectivité dispositif et notamment la protection des droits des personnes.

Elle a ainsi proposé un nouvel modèle de gouvernance. En effet, l'objectif est bien de garantir au citoyen un contrôle de proximité sur son territoire et de prendre en compte la nécessité d'un guichet unique pour les entreprises déployant des traitements transfrontières.

À cette fin, les autorités doivent rester compétentes pour exercer l'ensemble de leurs missions selon un double critère : l'établissement du responsable de traitement/sous-traitant ou le public ciblé.

La désignation d'une autorité chef de file sur la base du critère d'établissement principal, permet d'assurer l'organisation de la coopération entre les autorités compétentes. Cette autorité chef de file ne dispose pas de compétence exclusive, elle instruit et coordonne. Les décisions sont adoptées dans le cadre d'une procédure de codécision, avec l'accord des autres autorités concernées qui voient ainsi leur indépendance préservée. Le CEPD n'est alors saisi qu'en cas de désaccord entre les autorités ou pour garantir l'interprétation uniforme du règlement.

L'efficacité du système proposé tient au caractère contraignant de la décision finale ainsi qu'à la garantie d'un droit au recours effectif. En effet, puisque les décisions sont approuvées par les autorités compétentes, les personnes concernées peuvent introduire un recours devant leur juridiction administrative nationale contre les décisions de leur autorité lésant leurs intérêts. De même, pour les entreprises, celles-ci peuvent porter leurs recours devant les juridictions du pays de l'autorité chef de file.

Elle considère également qu'il est essentiel de maintenir un contrôle *a priori* sur les transferts, sur la base de règles clairement définies, et d'écarter la possibilité de recours à des instruments sans valeur juridique pour encadrer ces transferts.

La CNIL a poursuivi également ses échanges avec la Commission européenne, afin d'exposer ses préoccupations et sensibilisé la commission des affaires étrangères de l'Assemblée nationale et la commission des affaires européennes du Sénat. Par la suite, les deux assemblées ont exprimé dans une résolution européenne des réserves sur la proposition de règlement en ce qui concerne les règles de compétence, rejoignant la position exprimée par la CNIL. Les discussions avec le gouvernement français se sont également poursuivies tout au long de l'année 2012.

Éducation numérique/Les principales actions engagées par la CNIL

En 2012, la CNIL a décidé de faire de l'éducation au numérique une priorité stratégique en renforçant son action avec l'élaboration de nouveaux outils et l'élargissement de leur diffusion. Dans ce cadre, elle a mené plusieurs actions en 2012 :

- L'enrichissement du site dédié (jeunes.cnil.fr), sur lequel des fiches pédagogiques sont disponibles,
- La réalisation d'un serious game sur les réseaux sociaux
- La délivrance de label pour les « formations Informatique et Libertés ».
- La formation de formateurs tant auprès des associations de consommateurs que des chambres de commerce et d'industrie, relais des entreprises.

Le suivi des évolutions technologiques

Le cloud

À la suite de la consultation publique menée en 2011, la CNIL a publié en juin 2012 un ensemble de recommandations à destination des organismes qui souhaitent avoir recours à des prestations de cloud et notamment les PME.

Ces recommandations sont assorties de modèles de clauses contractuelles qui peuvent être insérés dans les contrats de services de *cloud computing* afin de couvrir les questions liées à la protection des données à caractère personnel.

Les compteurs communicants

La CNIL mène depuis plus de deux ans une réflexion sur ces compteurs et étudie notamment leur impact sur la vie privée des personnes. Au vu de ces risques pour la vie privée des personnes, la Commission a adopté en 2012, une première recommandation afin d'encadrer l'utilisation des compteurs communicants.

Cette recommandation, pose notamment comme principe que la courbe de charge ne peut être collectée de façon systématique, mais uniquement lorsque cela est justifié pour réaliser des travaux sur le réseau ou lorsque l'abonné en fait expressément la demande pour bénéficier de services particuliers.

Elle pose également un certain nombre d'exigences en termes de sécurité, des garanties sérieuses devant être apportées pour assurer la confidentialité des données (ex. : réalisation d'études d'impact sur la vie privée avant le déploiement des compteurs et d'analyses de risques pour déterminer les mesures techniques adéquates à mettre en place).

Google

Suite à l'annonce de Google en janvier 2012, de l'entrée en vigueur de nouvelles règles de confidentialité et de nouvelles conditions d'utilisation applicables à la quasi-totalité de ses services, la CNIL mandatée par le G29, a examiné ses nouvelles règles.

Dans le cadre de cette mission, elle a envoyé deux questionnaires à Google. Sur la base de l'analyse des réponses fournies et suite à l'examen de nombreux documents et mécanismes techniques, le G29 a formulé des recommandations sous la forme d'un courrier adressé à Google le 16 octobre 2012 et signé par les 27 autorités européennes de protection des données.

Actions de contrôle

La notification des violations de données à caractère personnel

À l'occasion de la révision des directives « Paquet télécom » en 2009, le législateur européen a imposé aux fournisseurs de services de communications électroniques l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées. Cette obligation a été transposée en droit français par l'ordonnance du 24 août 2011 son décret d'application du 30 mars 2012.

La CNIL s'est donc vue confier une nouvelle mission : elle doit apprécier le niveau de sécurité des systèmes des fournisseurs de services de communications électroniques, et les accompagner dans la mise en œuvre de mesures de protection efficaces contre toute violation de données. Elle peut enfin, en fonction de la gravité de cette violation, imposer aux fournisseurs l'information des personnes concernées.

De mars à décembre 2012, la CNIL a ainsi reçu une quinzaine de notifications.

Le traitement d'antécédent judiciaire (TAJ)

La CNIL a rendu un avis sur le projet de décret créant le traitement d'antécédents judiciaires. Ce fichier commun à la police et à la gendarmerie nationale a pour finalité de faciliter la constatation d'infractions, le rassemblement de preuves et la recherches des auteurs d'infractions.

S'il apporte de nouvelles garanties pour les personnes, il a également suscité quelques réserves de la part de la CNIL qui considère qu'il est indispensable de procéder à un important travail de mise à jour des données des fichiers originaux avant leur fusion.

Par ailleurs, fin 2012, la CNIL a mené un contrôle approfondi (20 contrôles sur place et 60 contrôles sur pièces) des fichiers d'antécédents judiciaires.

Organisation	Autorité française de protection des données
Président et/ou collège	Président : Isabelle FALQUE-PIERROTIN, Vice-présidents : Emmanuel de GIVRY, Jean-Paul AMOUDRY Composition du collège : 4 parlementaires / 2 membres du Conseil économique et social / 6 juges de la Cour suprême / 5 personnalités qualifiées désignées par le Conseil des ministres (3), par le président de l'Assemblée nationale (1) et par le président du Sénat (1).
Budget	Montant total des crédits pour 2012 (en millions d'EUR) : 17,2
Personnel	Effectif : 171
Activités générales	
Décisions, avis, recommandations	2 078 décisions (+ 5,5 % par rapport à 2011) / 113 avis / 2 recommandations
Notifications	88 990 notifications à la CNIL, dont : 8 946 notifications pour des systèmes de vidéosurveillance (+49,3 % par rapport à 2011) 5 483 notifications pour des systèmes de géolocalisation (+ 22,3 % par rapport à 2010)
Examens préalables	Autorisations : 1 534 en 2012, dont : 316 autorisations adoptées en séance plénière, 950 autorisations de transfert de données vers des États non membres de l'UE, 3 autorisations cadres, 795 autorisations de systèmes biométriques (+ 6,8 % par rapport à 2011), 658 autorisations de traitement de données à caractère personnel à des fins de recherche médicale, et 162 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 des personnes concernées	**Demandes émanant du public :** En 2012, la CNIL a reçu **35 924** demandes par écrit et **134 231** appels téléphoniques
Plaintes émanant des personnes concernées	La CNIL a reçu **6 017** plaintes en 2012 (+ 4,9 % par rapport à 2011). Il s'agit du nombre de plaintes le plus élevé qu'ait reçu la CNIL à ce jour. Ces plaintes portaient essentiellement sur le droit à l'oubli et les systèmes de vidéosurveillance. **Demandes émanant des personnes concernées : 3 682** demandes d'accès indirect dans le cas où le traitement des données concerne la sécurité de l'État, la défense nationale ou la sécurité publique (+ 75 % par rapport à 2011).
Conseils sollicités par le Parlement ou le gouvernement	**En 2012,** la CNIL a adopté **113 avis**. La CNIL a par ailleurs rencontré et été **auditionnée à 22** reprises par des membres du Parlement français pour un échange de vues sur des questions de protection des données.
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	**458** enquêtes (+ 19 % par rapport à 2011), dont **173** enquêtes relatives à des systèmes de vidéosurveillance.
Activités de sanction	
Sanctions	**13 sanctions prises par la CNIL en 2012.** **Actions en justice à l'encontre des responsables de données : 56 (43** mises en demeure, **4** amendes, **9** avertissements), **2** décharges.
Amendes	Amendes imposées par la CNIL **en 2012** pour un **montant total de 16 001 EUR**
DPD	
Chiffres relatifs aux DPD	**10 709** organisations ont désigné un DPD (+ 24 % par rapport à 2011).

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.

- Ccass, chambre sociale M G c/ Société Groupe Progrès 10208450 (4/04/2012)
- Ccass, chambre civile 2 M X c/ Nouvelle du Journal de l'Humanité (12/04/2012)

- Ccass, chambre civile, Aufeminin.com c/ Google France 1115188 (12/07/2012)
- Ccass, chambre civile Google France c/ Bac films (12/06/2012)
- Ccass, chambre commerciale, financière et économique eBay Inc, eBay International c/ LVMH et autres (03/05/2012)
- Ccass, chambre criminelle Damien 1180801 (06/03/2012)
- Ccass, chambre sociale Boymond c/ Société Technique française du nettoyage 1023482 (10/01/2012)
- Ccass, chambre sociale M G c/ Société Groupe Progrès 1020845 (04/04/2012)
- Ccass, chambre sociale M X c/ Association Perce-neige (10/05/2012)
- Ccass, chambre sociale M. X c/ Nouvelle communication téléphonique (10/05/2012)
- Ccass, chambre sociale M X c/ SAS Helpevia1115310 (26/06/2012)
- Ccass, chambre sociale Mme X c/ Société Réunion fixations 1023521 (23/05/2012)

GRÈCE

A. Résumé des activités et actualités :

Le Parlement hellénique a adopté la loi 4070/2012 qui, notamment, transpose la directive 2009/136/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Par ailleurs, et conformément au 15e rapport annuel du groupe de travail « Article 29 » sur la protection des données, le Parlement hellénique a adopté la loi 4055/2012, qui comprend certaines dispositions régulant des sujets liés à l'exploitation des autorités indépendantes protégées par la constitution en général, et l'autorité de protection des données (ci-après l'AHPD) en particulier.

Une fois de plus, néanmoins, le sérieux problème de manque de personnel, que l'AHPD a connu dès sa création, n'a pas pu être résolu au cours de l'année 2012 en raison de la situation actuelle 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.

Au total, l'AHPD a émis cette année 194 décisions et 5 avis (dont certains sont brièvement présentés à la section B, Informations sur la jurisprudence).

L'AHPD a en outre exprimé par écrit son point de vue sur a) la création d'un Registre des citoyens intégré correspondant à l'interconnexion des registres du ministère des Finances, du travail et de la sécurité sociale, du ministère de l'Ordre public et de la protection des citoyens et du ministère de l'Intérieur, b) le nouveau cadre des services d'administration en ligne, c) le projet de règlement sur les signatures électroniques et autres services de confiance abrogeant la directive 1999/93/CE et d) le nouveau cadre juridique sur la protection des données à caractère personnel, et a été invitée à une audience parlementaire.

À l'occasion de la Journée européenne de la protection des données 2012, l'AHPD a par ailleurs ajouté de nouvelles rubriques à son site Internet, en a révisé le contenu en profondeur et amélioré l'intégralité de la structure. À des fins de sensibilisation, l'Autorité a également lancé un bulletin d'informations sur l'évolution actuelle du domaine des données à caractère personnel aux niveaux national, européen et international. Pour finir, afin de planifier de nouvelles activités d'aide sociale, l'AHPD a créé et réalisé une enquête en ligne (sur son site Internet) sur des questions liées à la protection des données à caractère personnel.

Organisation	Autorité hellénique de protection des données
Président et/ou collège	Petros Christoforos (Président du collège).
Budget	2 213 787 EUR
Personnel	Département des contrôleurs : 15 avocats et 11 experts informatiques (dont trois (3) en congé sans solde et un (1) démissionnaire), Département des communications et des RP : 5 (dont deux (2) détachés une partie de l'année auprès d'autres organismes / agences de la fonction publique, une (1) en congé maternité), Département des ressources humaines et des finances : 16 (dont un

	(1) transféré vers un autre organisme de la fonction publique).
Activités générales	
Décisions, avis, recommandations	Au total, l'AHPD a formulé 194 décisions et 5 avis.
Notifications	L'AHPD a reçu 540 notifications (335 concernant l'installation et le fonctionnement de caméras de télésurveillance et 57 transferts de données vers des pays en dehors de l'UE).
Examens préalables	L'AHPD a émis ou renouvelé 81 autorisations concernant le traitement de données sensibles, l'interconnexion de fichiers et le transfert de données vers des pays tiers sans un niveau de protection adéquat.
Demandes émanant des personnes concernées	989
Plaintes émanant des personnes concernées	675 (autorités judiciaires et policières nationales : 8, défense nationale : 1, administration publique et gouvernement local : 24, services fiscaux, ministère des finances : 6, santé : 13, sécurité sociale : 4, éducation et recherche : 4, banques : 75, secteur privé : 64, communications électroniques : 254, relations professionnelles : 20, moyens de communication de masse : 23, autres : 179).
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 2012, l'AHPD a ajouté de nouvelles rubriques à son site Internet (« autorités policières – sécurité », « fiscalité », « sécurité sociale », « nouvelles technologies », « éducation – recherche », « santé » et « finance »), en a révisé l'intégralité du contenu et amélioré la structure. À des fins de sensibilisation, l'Autorité a créé un bulletin d'informations sur l'évolution actuelle du domaine des données à caractère personnel aux niveaux national, européen et international. Afin de planifier de nouvelles activités d'aide sociale, l'AHPD a créé et réalisé une enquête en ligne (sur son site Internet) sur des questions liées à la protection des données à caractère personnel.
Activités d'inspection	
Contrôles, enquêtes	11 contrôles (dont 10 auprès de responsables du traitement des données du secteur privé et, plus particulièrement, de sociétés déployant des activités d'achat / vente de bases de données contenant des données à caractère personnel, 1 auprès de la représentation nationale du SIRENE et du Système d'information Schengen (SIS)). Deux (2) inspections spéciales ont été réalisées sur le fonctionnement de systèmes de vidéosurveillance au sein d'une société et d'une ONG. Quatre (4) autres inspections qui avaient débuté en 2011 ont été complétées en 2012 (3 sur la protection et

	la sécurité des données à caractère personnel détenues et traitées par les services et systèmes électroniques spécifiques du ministère de l'Éducation (voir la jurisprudence), 1 sur le système de prescription en ligne du secrétariat général de la sécurité sociale, du ministère de l'Emploi et de la protection sociale.
Activités de sanction	
Sanctions	38 sanctions (5 avertissements, 33 amendes) ont été imposées par la DPA dans les domaines thématiques suivants : secteur public (1), santé (5), européen-international (1), secteur financier (14), violations des données à caractère personnel (8), moyens de communication de masse (3), éducation et recherche (1) et communications électroniques (4). Dans trois décisions, l'AHPD a imposé un avertissement et une amende.
Amendes	Amendes : Montants : 2 500 à 50 000 EUR (total 486 500 EUR) ont été imposés par l'AHPD.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Avis 3/2012

Un avis a été formulé par l'AHPD concernant les exigences de saisie et de suppression des étrangers sur la base de l'article 96 de l'Accord de Schengen et du registre national des étrangers indésirables. L'Autorité a jugé que saisir un étranger dans le registre national n'entraîne pas une alerte *ipso jure* dans le SIS. La saisie d'un étranger dans le SIS se fait en vertu des exigences de l'article 96 de l'Accord de Schengen. L'expulsion par les autorités administratives ou judiciaires en conformité avec le droit national justifie une alerte au niveau du registre national et du SIS. Un étranger est saisi dans le SIS si il ou elle a été reconnu coupable par un tribunal national d'une infraction passible d'une privation de liberté d'au moins un (1) an. La saisie d'un étranger dans le SIS est justifiée s'il existe des motifs sérieux de penser que la personne concernée a commis ou a l'intention de commettre de graves infractions pénales. La saisie d'un étranger dans le registre national est également justifiée en cas d'expulsion administrative basée sur des fondements spécifiques et si la présence de l'étranger est légitimement dangereuse pour l'ordre public et la sécurité du pays. Les données d'un étranger sont effacées du SIS après une période de trois ans à compter de l'alerte et en l'absence de décision justifiée de les conserver.

Décision 36/2012

L'AHPD a estimé que la publication dans un journal d'une photographie montrant, sans leur consentement préalable, une mère et sa fille en bas âge dans le contexte d'un article sur l'endométriose constitue un traitement, une collecte et une conservation de données à caractère personnel illégaux. L'Autorité a conclu que la photographie était sans objet quant au contenu de l'article et pouvait créer l'impression, pour le lecteur moyen, que la mère souffrait de la condition susmentionnée. Elle a imposé une amende au responsable du traitement, ordonné la suppression de ces données des archives du journal et interdit leur republication.

Décision 112/2012

L'AHPD a examiné un certain nombre de notifications concernant les services de géolocalisation (utilisant la technologie GPS) et de surveillance 24 heures sur 24 fournis par deux sociétés. Les abonnés à ces services peuvent déterminer les fonctionnalités du service et la position géographique du détenteur de l'appareil de géolocalisation. Ces services s'adressent, notamment, aux personnes ayant des problèmes de santé ou tenus de s'occuper de personnes ayant des problèmes de santé, ainsi qu'aux parents de mineurs, pour des raisons de sécurité personnelle. Le traitement des données du détenteur de l'appareil comprend le traitement des données de géolocalisation, de données démographiques et de données de santé sensibles. La décision de l'AHPD fixe des conditions spécifiques pour la protection des données à caractère personnel qui découlent de ces services de géolocalisation et, notamment, les suivantes : le responsable du traitement doit fournir des informations adéquates au détenteur de l'appareil sur le traitement des données de ce dernier, l'accès à ces données et les mesures de sécurité mises en œuvre ; dans certains cas, les données doivent être cryptées et/ou protégées par des mesures de sécurité ; en outre, le détenteur de l'appareil doit avoir été avisé et avoir préalablement donné son consentement ; par ailleurs, pour les données sensibles, ce consentement doit avoir été donné par écrit ; si le détenteur de l'appareil est une personne frappée d'incapacité légale, le consentement doit être donné par le tuteur à l'instance ; pour les mineurs, le consentement doit être donné par les parents / tuteurs, mais l'avis du mineur doit être pris en compte ; le détenteur de l'appareil doit pouvoir exercer son droit de refus ; l'utilisation de ce système avec des mineurs doit d'abord être évaluée, en termes de risque, par les autorités publiques compétentes et, en attendant, doit être limitée aux raisons de santé.

Décision 117/2012

Une organisation politique a publié une affiche montrant en arrière-plan (sans leur consentement) un groupe de personnes protestant dans une manifestation. L'AHPD a jugé que cette photo d'un groupe de personnes n'avait pas de lien direct avec le contenu de l'affiche et pouvait laisser penser de manière erronée au citoyen moyen que ces personnes étaient des sympathisants de ladite organisation politique. L'Autorité a par conséquent imposé une sanction à l'organisation, interdit la republication de l'affiche et ordonné sa suppression.

Décision 165/2012

L'Autorité a jugé que la publication de données à caractère personnel sensibles (concernant des poursuites pénales) dans l'édition électronique d'un journal (sur son site Internet) contrevient à la loi 2427/1997 sur la protection des données à caractère personnel. Plus particulièrement, l'AHPD a jugé que la publication illégale de données à caractère personnel sensibles sur Internet (via un moteur de recherche) enfreint de manière disproportionnée les droits de la personne concernée parce que l'utilisation de ce type de traitement associe toujours la personne concernée à un comportement passé et que, par conséquent, ces informations deviennent facilement accessibles à quiconque en fait la recherche (et pas seulement les journalistes, les chercheurs et les universitaires). L'AHPD a par ailleurs imposé une amende au responsable du traitement, ordonné que les données concernant la personne concernée publiées sur le site du journal soient rendues anonymes, de sorte que même en cas de recherche par date de publication, il ne soit plus possible d'identifier la personne concernée, et a formulé un avertissement (adressé au responsable du traitement) afin d'examiner le droit de la personne concernée de s'opposer et de rendre anonymes les données ou de rejeter les plaintes en donnant des raisons spécifiques.

Décision 187/2012

L'AHPD a adressé un avertissement au ministère de l'Éducation afin de faire respecter les recommandations spécifiées dans son rapport après la réalisation de trois contrôles des systèmes électroniques de « service électronique d'émission de tickets spéciaux / de cartes d'identité pour étudiants », d'« enseignement en ligne » et de « centre de données en ligne » concernant la protection et la

sécurité des données à caractère personnel détenues et traitées par ces systèmes. L'Autorité a notamment identifié des déficiences spécifiques et/ou des omissions de la part du responsable du traitement dans les procédures et l'organisation de la sécurité, la documentation suffisante des mesures de sécurité appliquées et leur contrôle systématique, l'authentification des utilisateurs, la gestion et le soutien de ces systèmes et, enfin, les obligations générales relevant de la loi 2472/1997.

HONGRIE

A. Résumé des activités et actualités :

Organisation	Autorité nationale pour la protection des données et la liberté d'information
Président et/ou collège	Dr Attila Péterfalvi
Budget	390 211 000 HUF
Personnel	59
Activités générales	
Décisions, avis, recommandations	2 152 (protection des données : 1 825, liberté d'information : 327)
Notifications	12 166
Examens préalables	Les enquêtes d'audit sur la protection des données sont autorisées par la loi du 1er janvier 2013.
Demandes émanant des personnes concernées	1 388 (protection des données : 1 212, liberté d'information : 176)
Plaintes émanant des personnes concernées	764
Conseils sollicités par le Parlement ou le gouvernement	207 + 46 (incitations à des amendements juridiques)
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	2 152
Activités de sanction	
Sanctions	
Amendes	11
DPD	
Chiffres relatifs aux DPD	Organisation de la conférence des DPD (juin 2012)

B. Informations sur la jurisprudence

B1) Traitement illicite de données – opérateur de sites web (www.ingatlandepo.com et www.ingatlanbazar.com)

La DPA hongroise a imposé une amende (de 10 000 000 HUF, soit le montant actuellement le plus élevé autorisé par la loi) à un opérateur de sites web (ci-après le « défendant »). Des contrats ont été conclus entre des personnes concernées hongroises (ci-après les « plaignants ») et le défendant dans le but d'assurer la publicité de biens immobiliers au nom des plaignants sur le site web du défendant.

Une fois les biens immobiliers vendus, les publicités expirées ou si les plaignants souhaitaient simplement les supprimer ou demander au défendant de les supprimer, ce dernier ne le faisait pas. Malgré les demandes insistantes des plaignants, le défendant n'a jamais effacé les publicités. Le défendant a par ailleurs communiqué les données personnelles des plaignants à des sociétés de gestion des réclamations, entre autres.

De nombreuses plaintes ont été reçues par la DPA hongroise en raison des problèmes susmentionnés. La DPA a par conséquent lancé une procédure d'enquête et appelé le défendant à faire des déclarations sur son comportement dans un certain délai. Le défendant n'ayant pas coopéré dans le délai imparti par la DPA et ayant apporté la preuve de sa réticence à coopérer, la DPA a lancé une procédure de protection des données.

En conséquence de cette procédure, la DPA a conclu que le défendant avait violé le droit à la vie privée des plaignants en de multiples occasions. Le défendant a notamment enfreint le principe de proportionnalité, le droit à l'information, le droit des personnes concernées de supprimer leurs données personnelles ou de les faire supprimer par le responsable du traitement des données, ainsi que le principe de limitation de la finalité. Le responsable du traitement des données a par ailleurs ignoré les multiples objections des plaignants par rapport au traitement des données par le défendant. Par conséquent, les différentes activités de traitement des données du défendant ne reposaient sur aucun fondement juridique essentiel.

En conséquence et compte tenu du nombre de personnes affectées par l'infraction, de sa gravité, de son caractère répété et de la réticence du défendant à coopérer avec les autorités publiques compétentes et les parties concernées, l'Autorité a décidé d'imposer une amende et de divulguer sa décision de protéger les droits d'un plus grand nombre de personnes concernées.

Le cas est encore en attente d'une décision.

B2) Google Street View (GSV)

Suite aux nombreuses consultations des représentants de Google Inc. (prestataire des services de GSV) et à plusieurs enquêtes menées par l'ancien commissaire à la protection des données en 2009 et compte tenu des récents jugements (C-468/10. et C-469/10.) rendus par la Cour de justice de l'UE, la NAIH a publié une déclaration approuvant le lancement des services de GSV en Hongrie sous réserve que Google respecte les principes de protection des données applicables et les conditions préalables (y compris, notamment, de notification préalable au public ; de permettre aux personnes concernées de soumettre des demandes de suppression ; de flouter les données à caractère personnel dès que possible, etc.) énoncés par la NAIH dans sa déclaration.

B3) Application de systèmes de vidéosurveillance sur les lieux de travail

De nombreuses pétitions ont été reçues par la NAIH et l'ancien commissaire à la protection des données ces dernières années, dont les auteurs se plaignaient de l'application trop répandue de systèmes de vidéosurveillance sur les lieux de travail.

Depuis 2012, l'ancien Code du travail et la loi sur la protection des données de 1992 ont été remplacés par de nouveaux instruments juridiques. Le nouveau Code du travail, entré en vigueur le 1er juillet 2012, inclut déjà des dispositions (§§ 9 et 11) qui doivent être prises en compte pour les systèmes de vidéosurveillance sur les lieux de travail. Ces dispositions générales peuvent néanmoins donner lieu à différents modes d'application du droit à l'autodétermination informationnelle.

Suite à une enquête approfondie, nous avons publié une recommandation dans laquelle nous proposons des lignes directrices aux employeurs dans l'objectif de faire respecter les exigences légales en matière de protection des données sur les lieux de travail.

B4) Identification biométrique

Un client a demandé à l'Autorité de lui fournir une déclaration officielle établissant si le traitement des données d'une école pouvait être licite en cas d'intention de l'établissement d'installer un système d'identification biométrique au niveau de ses entrées.

Considérant les réglementations nationales et européennes applicables, le client a été conseillé comme suit.

Les empreintes digitales d'une personne physique sont considérées comme des données à caractère personnel et la prise d'empreintes digitales est considérée comme une forme de traitement de données. La législation nationale applicable et la directive européenne relative à la protection des données stipulent les principes juridiques fondamentaux qui doivent également être pris en compte dans le cadre d'activités de traitement des données. Ceux-ci comprennent par exemple le principe de proportionnalité (et al.).

L'Autorité a conclu qu'un système biométrique (visant à prendre les empreintes digitales des élèves à l'entrée de l'école) à des fins de sécurité personnelle et de protection d'une propriété ne respecte pas les exigences de proportionnalité. Une meilleure identification pourrait être assurée par d'autres moyens plus inoffensifs et moins intrusifs envers la vie privée.

Par conséquent, l'introduction d'un système d'entrée de ce type remettrait en cause le droit à la vie privée des personnes concernées.

B5) Informatique en nuage

Une association politique a saisi l'Autorité d'une requête lui demandant une déclaration sur la légalité des activités de traitement des données de l'association. L'association (ci-après le « responsable du traitement ») a indiqué son souhait de traiter les données à caractère personnel de ses sympathisants en employant la technologie de l'informatique en nuage. Elle a ajouté avoir prévu de choisir un prestataire de services d'informatique en nuage dont la société mère est enregistrée aux États-Unis et ayant une filiale en Irlande. Le prestataire de services en question figure sur la liste relative à la sphère de sécurité publiée par le Département du commerce des États-Unis.

L'Autorité a conclu que la nature sensible des données à caractère personnel des sympathisants d'une association active sur le plan politique entraînait une augmentation significative des préoccupations de sécurité. C'est pourquoi l'Autorité s'est opposée au transfert de ces données à caractère personnel dans le« nuage ».

B6) Piratage du site Internet de Capital Mineral Water and Beverage Co. Ltd.

En octobre 2012, un groupe de pirates informatiques turcs a déclaré avoir compromis le site Internet promotionnel de la société susmentionnée. Résultat : plus de 50 000 éléments de données à caractère personnel (noms, adresses électroniques, dates de naissance, etc.) ont été volés. À cette occasion, notre Autorité a publié une annonce demandant pourquoi des données à caractère personnel de clients avaient

été rendues accessibles en ligne et pourquoi elles n'avaient pas été cryptées. Nous avons par la même occasion appelé à mieux considérer les mesures à introduire et à appliquer pour la sécurité des données afin d'éviter des violations similaires de données.

À cet égard, une procédure administrative de protection des données est encore en cours.

B7) Amende financière envers une société d'édition en ligne

Nous avons reçu une plainte d'une personne déclarant recevoir des courriels marketing non sollicités de la part d'une société à laquelle elle n'avait pas donné son consentement et indiquant que la société n'avait pas mis un terme à ses agissements ni effacé les coordonnées du plaignant malgré ses demandes répétées.

Suite à une enquête et à une procédure administrative de protection des données ultérieure, l'Autorité a imposé une amende financière de 3 millions de HUF. Ce montant colossal a été décidé en raison des circonstances aggravantes suivantes : l'étendue des personnes affectées par ce traitement illicite, le grand nombre de mineurs concernés, la gravité de l'infraction et la durée exceptionnelle de la situation d'illégalité. Des circonstances atténuantes ont également été prises en compte comme suit : la finalisation d'une nouvelle politique en matière de respect de la vie privée, son accessibilité sur le site Internet et le compte rendu des amendements dans le registre de la protection des données. Cette volonté du responsable du traitement de coopérer avec l'Autorité a été démontrée par la rapidité avec laquelle le responsable du traitement a apporté les modifications nécessaires juste après que la procédure de protection des données a été initiée.

B8) Traitement de données de sites de rencontres

La NAIH a enquêté sur un cas où une société hongroise (ci-après la « société »), un opérateur d'une quarantaine de sites, a dû payer une amende pour la protection des données de 3 millions de HUF principalement en raison de la violation des droits de mineurs et d'activités de traitement illégal de données liées, notamment, aux services de marketing par courriel offerts. Ce cas a été ouvert suite à la plainte d'un citoyen à l'encontre de la société dont il a déclaré qu'elle lui adressait des courriels contenant des publicités de manière continue et sans son consentement, qu'elle n'avait pas effacé ses coordonnées après qu'il le lui avait demandé et qu'elle avait même continué de lui envoyer son bulletin d'information.

Dans le cadre de ses procédures, la NAIH s'est aperçue que, sur les sites Internet gérés par la société, les détails relatifs au traitement des données, y compris au transfert à des tierces parties des données saisies lors de l'inscription, n'étaient pas clairs. Aucune possibilité n'était garantie aux utilisateurs de pouvoir donner leur consentement libre et éclairé de recevoir des courriels de marketing, car ce consentement était considéré comme automatique avec l'inscription. La NAIH a par ailleurs montré que les informations fournies sur l'objet du traitement des données étaient inadéquates et que les utilisateurs n'avaient aucune possibilité de se désabonner des bulletins d'information envoyés par la société. Lors de son enquête, la NAIH a par ailleurs identifié un autre problème relativement inquiétant, à savoir l'inscription mal gérée de mineurs, particulièrement sur des sites de rencontres.

Les bases juridiques sur lesquelles la NAIH a fondé sa décision sont la loi CXII de 2011 sur l'autodétermination informationnelle et la liberté d'information, la loi XLVII de 2008 sur l'interdiction des pratiques commerciales déloyales envers les consommateurs, la loi CVIII de 2001 sur le commerce électronique et la loi IV de 1959 sur le Code civil. La NAIH a également tenu compte des conclusions des avis 5/2004, 5/2009 et 15/2011 du groupe de travail « Article 29 » sur les réseaux sociaux, de la recommandation 2006/952/CE du Parlement européen et du Conseil du 20 décembre 2006 sur la protection des mineurs et de la dignité humaine et sur le droit de réponse en lien avec la compétitivité de l'industrie européenne des services audiovisuels et d'information en ligne, et du rapport COM(2011) 556 de la Commission européenne sur la protection des enfants dans le monde numérique.

La NAIH, parmi d'autres problèmes de moindre importance, a conclu sa procédure administrative en déclarant que les activités de traitement de données de la société n'étaient pas en harmonie avec les actes législatifs et non législatifs susmentionnés et mettaient sérieusement en danger le droit des mineurs à la protection en omettant complètement de demander le consentement nécessaire aux représentants légaux (parents) des mineurs. La société a en outre violé le droit des personnes concernées à la protection des données en ne leur assurant pas la possibilité d'une procédure adéquate à l'inscription, lorsqu'un consentement libre et éclairé devrait leur être demandé pour le transfert de leurs coordonnées électroniques à des fins marketing et d'envoi de courriels marketing. Elle ne les a par ailleurs pas clairement informées sur les règles et procédures de protection des données et ne leur a pas donné la possibilité de se désabonner du bulletin d'information de la société. Concernant les pratiques de la société en matière de courriels marketing, la NAIH a suggéré dans le cadre de ses délibérations l'emploi d'une solution d'abonnement en vertu de laquelle une case à cocher distincte et spécifique serait proposée à l'inscription.

B9) Traitement de données par un système d'achats à tarifs réduits

La NAIH a reçu une plainte d'une personne physique dans le cadre d'une activité de traitement de données prétendument abusive de la part d'une société de marketing (ci-après la « société »). La société gérait un système de cartes de réduction en vertu duquel les membres inscrits pouvaient acheter des articles à des tarifs inférieurs auprès de certains entrepreneurs. L'inscription dans le système était possible exclusivement sur invitation d'un membre déjà inscrit. Les membres actifs bénéficiaient de réductions pour avoir recruté de nouveaux membres. L'Autorité a ensuite reçu des plaintes de membres déclarant que le système ne fonctionnait pas conformément aux règles de protection des données applicables. L'Autorité a tout d'abord lancé une procédure d'enquête afin de mieux comprendre les faits. Le responsable du traitement des données ayant omis de répondre à plusieurs demandes, la NAIH a décidé d'initier une procédure administrative de protection des données. À l'issue de ses procédures, la NAIH a conclu que le responsable du traitement ne disposait pas d'une politique exhaustive et simple à comprendre en matière de respect de la vie privée, ce qui empêchait ses clients d'avoir connaissance de leurs droits et de donner librement leur consentement au traitement de leurs propres données à caractère personnel par le responsable du traitement.

C. Autres informations importantes

Modifications importantes de la législation

En conséquence d'une évolution fondamentale de la structure constitutionnelle de la Hongrie, suite à une décision de l'Assemblée nationale hongroise en 2011, l'ancien bureau du commissaire à la protection des données a été fermé et un nouvel organisme, appelé Autorité nationale pour la protection des données et la liberté d'information, a été chargé des responsabilités susmentionnées et a commencé à travailler le 1er janvier 2012. Le nouvel instrument juridique ayant vocation à régir les domaines de la protection des données et de la liberté d'information, la Loi CXII de 2011 sur le droit à l'autodétermination informationnelle et la liberté d'information, a été adoptée par le Parlement le 11 juillet 2011 et est entrée en vigueur le 1er janvier 2012.

Certaines dispositions de la nouvelle loi hongroise sur la vie privée (loi CXII de 2011 sur le droit à l'autodétermination informationnelle et la liberté d'information, entrée en vigueur le 1er janvier 2012) régissant le mandat du président de la DPA hongroise (ci-après le « président »), considérant également les remarques critiques de la Commission européenne, ont été modifiées en profondeur de manière à renforcer l'indépendance de la position du président (loi modificative : loi XXV de 2012). Ci-dessous sont spécifiés les amendements apportés en conséquence.

- Dans les cas où la conclusion relative à la cessation du mandat de président serait reconnue par le Président hongrois en vertu d'une motion écrite du Premier Ministre, le président aurait le droit de faire appel de cette motion devant un tribunal. Le recours sera introduit contre le Premier Ministre. La raison de cette modification est que le mandat du président ne cessera que si la motion du Premier Ministre est sans aucun doute licite et bel et bien fondée sur des faits réels.
- Cette modification autorise le président à participer et à s'adresser aux sessions des comités parlementaires, ce qui l'habilite de fait à informer les députés de ses activités et à faire des suggestions concernant le processus législatif et les projets de lois.
- Un autre amendement stipule que le président aura (en plus d'autres conditions supplémentaires) au moins dix ans d'expérience professionnelle en matière de supervision de procédures liées à la protection des données ou à la liberté d'information. En vertu des anciens règlements, cinq ans d'expérience professionnelle suffisaient.

IRLANDE

A. Résumé des activités et actualités :

En 2012, le bureau du commissaire à la protection des données a ouvert 1 349 dossiers de plaintes formelles à des fins d'enquête (de nombreuses plaintes sont traitées de manière informelle en fournissant au plaignant les informations appropriées quant à ses droits). 864 enquêtes sur des plaintes ont été conclues en 2012. Comme les années précédentes, la grande majorité des plaintes ont été réglées à l'amiable, 36 plaintes seulement donnant lieu à des décisions formelles. Les premières poursuites ont été engagées contre des sociétés de télécommunication ayant omis de respecter les nouvelles exigences de sécurité et de notification de violation découlant du 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). Les informations relatives aux poursuites engagées en 2012 figurent à la section B du présent rapport. Le nombre de notifications d'atteintes à la sécurité de données à caractère personnel adressées au bureau a continué d'augmenter (1 592 en 2012), une tendance qui fait suite à l'introduction du Code de bonnes pratiques en matière d'atteintes à la sécurité des données à caractère personnel en 2010.

Organisation	Bureau du commissaire à la protection des données
Président et/ou collège	Billy Hawkes
Budget	1 458 000 EUR. 1 552 468 EUR dépensés.
Personnel	28 au 31 décembre 2012.
Activités générales	
Décisions, avis, recommandations	36 décisions formelles.
Notifications	5 338
Examens préalables	s. o.
Demandes émanant des personnes concernées	9 500 demandes par courriel. Demandes également reçues par écrit.
Plaintes émanant des personnes concernées	1 349
Conseils sollicités par le Parlement ou le gouvernement	Consultations informelles régulières sur des propositions législatives / réglementaires.
Autres renseignements relatifs aux activités générales	1 592 notifications d'atteintes à la sécurité des données à caractère personnel.
Activités d'inspection	
Contrôles, enquêtes	40 audits (contrôles)

Activités de sanction	
Sanctions	195 poursuites engagées contre 11 entités.
Amendes	7 500 EUR d'amendes imposées plus les coûts. 99 500 EUR de dons caritatifs ordonnés par le tribunal par le biais de l'application de la loi sur les probations, plus les coûts.
DPD	
Chiffres relatifs aux DPD	s. o.

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 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 concerné à la personne concernée ou à une œuvre caritative appropriée. Lorsque nécessaire, des pouvoirs coercitifs sont appliqués, par exemple lorsque les responsables du traitement de données ne respectent pas les droits d'accès des personnes concernées. Dans certains cas, les responsables du traitement de données sont nommés dans des études de cas incluses dans le rapport annuel du commissaire. Au cours de l'année 2012, le commissaire a entamé avec succès plusieurs actions en justice en rapport avec les droits conférés aux personnes concernées par les lois de 1988 et de 2003 sur la protection des données et le décret-loi 336 de 2011 (transposant la directive 2002/58/CE, telle qu'amendée par les directives 2006/24/CE et 2009/136/CE en Irlande). 195 poursuites ont été engagées à l'encontre de 11 entités en 2012. Celles-ci comprennent les premières poursuites engagées contre des sociétés de télécommunication ayant omis de respecter les nouvelles exigences de sécurité et de notification de violation découlant du décret-loi 336 de 2011, plusieurs poursuites relatives à des messages textes et courriels de marketing non sollicités, et des délits liés aux inscriptions et découlant des lois sur la protection des données.

La Haute Cour a également statué sur un appel relatif à un point de droit concernant l'accès aux données en cas de procédures judiciaires entre les parties. La Haute Cour a statué ce qui suit : « l'existence de procédures judiciaires entre un demandeur de données et le responsable du traitement des données n'empêche pas le demandeur de données de déposer une demande d'accès en vertu de la loi ni ne justifie que le responsable du traitement refuse cette demande ». Dans un autre appel devant la Haute Cour, celle-ci a maintenu la décision du commissaire de ne pas enquêter sur une plainte qu'il jugeait « futile ou contrariante » et confirmé ne pas avoir la compétence d'instruire un appel, dans la mesure où aucune enquête n'avait eu lieu.

C. Autres informations importantes

Le commissaire a poursuivi son engagement auprès des grandes organisations du secteur public sur l'ampleur du partage des données dans le secteur public. Un rapport sur l'enquête du bureau sur INFOSYS, un système de partage de données dans le secteur public irlandais, a été publié en annexe du rapport annuel de 2012 du bureau. L'enquête a révélé un échec de gouvernance dans certaines des organisations du secteur public auditées, et des recommandations d'amélioration de la gouvernance ont été formulées, en faveur, notamment, d'une transparence accrue et d'un accès et de contrôles de sécurité améliorés.

En reconnaissance des responsabilités accrues qui devraient incomber au bureau, lorsque les propositions législatives sur la protection des données actuellement en discussion au Conseil des Ministres de l'Union européenne et au Parlement européen auront eu force de loi, des membres du personnel supplémentaires ont été alloués au bureau fin 2012. Ces ressources comprennent un conseiller technologique en chef et un conseiller juridique, ainsi que des membres du personnel administratif supplémentaires. L'allocation du budget hors salaires du bureau pour 2013 a également été revue à la hausse.

ITALIE

A. Résumé des activités et actualités :

Le nouveau panel collégial de la DPA italienne est entré en fonction le 19 juin 2012, remplaçant le panel dirigé par le Prof. Francesco Pizzetti (2005-12). La nouvelle commission comprend M. Antonello Soro, président, Mme Augusta Iannini, vice-présidente, Mme Giovanna Bianchi Clerici et le Prof. Licia Califano, membres. M. Giuseppe Busia est le nouveau secrétaire général de la DPA.

Modifications de la législation

Communications électroniques – Notification d'une violation de données

La directive 2009/136/CE a été transposée en droit italien au cours de l'année 2012. En particulier, le décret législatif n° 69/2012 a introduit le concept de « violation de données à caractère personnel » dans le droit italien et défini les obligations des prestataires de services de communications électroniques accessibles au public en cas de violation (cf. section 32 a du code de protection des données italien).

Les autres modifications de la législation dans ce contexte concernent les amendements apportés à quelques définitions contenues dans le code de protection des données (la formulation « partie contractante » a remplacé « abonné »), les règles de stockage et d'accès aux informations sur l'équipement terminal de la partie contractante en ce qui concerne, notamment, les « cookies » (section 122 du code de protection des données), les mesures et procédures de sécurité que les prestataires de services de communications électroniques accessibles au public doivent mettre en œuvre (visées aux sections 32 et 132 a du code de protection des données) et les amendements correspondants apportés aux sanctions applicables (en vertu de la section 162 b relative aux « violations de données à caractère personnel »).

Mesures de « simplification »

La législation sur la protection des données a également fait l'objet de changements apportés par des mesures de « simplification » adoptées en urgence par le gouvernement italien (via un décret publié le 9 février 2012, adopté avec plusieurs amendements supplémentaires via la loi n° 35 du 4 avril 2012). Concernant, en particulier, les mesures de sécurité, le décret a remplacé l'obligation des responsables du traitement des données de rédiger un « document de politique de sécurité » par une déclaration autocertifiée. Toujours en vertu du décret en question, la DPA italienne a été privée de son pouvoir de fixer des arrangements simplifiés pour la mise en œuvre de mesures de sécurité minimales via des mesures propres.

Le même décret permet le traitement de données judiciaires conformément aux protocoles d'accord conclus par les organisations avec le ministère des Affaires intérieures (ou ses bureaux périphériques) afin de prévenir et de contrer le crime organisé, sous réserve que les catégories des données traitées et les opérations de traitement à exécuter soient clairement énoncées (cf. sections 21(1 a) et 27 du code de protection des données).

« Déclenchement d'alerte »

En vertu de la nouvelle section 54 a du décret législatif n° 165/2001 (« Protection des employés publics signalant des pratiques illicites »), un employé public ayant connaissance de pratiques illicites dans le cadre de la réalisation de tâches et signalant ladite conduite aux autorités judiciaires, à la Cour des comptes et/ou à son supérieur ne peut être puni ou licencié, ni faire l'objet de mesures discriminatoires impactant ses conditions professionnelles pour quelque motif que ce soit en relation avec ledit signalement.

Principales questions abordées

Les principales questions abordées par la DPA en 2012 comprennent des sujets qui ont été portés à son attention à plusieurs reprises au fil des ans. Les garanties pour les personnes concernées en termes de télémarketing, de déploiement de matériel (intelligent) de vidéosurveillance respectueux de la vie privée et de questions d'emploi telles que l'utilisation de données biométriques pour le contrôle des accès (considérée comme excessive et disproportionnée en comparaison des objectifs spécifiques) étaient au cœur des principaux cas traités en 2012. Une synthèse d'autres questions contenant des éléments de nouveauté est proposée ci-dessous.

Violations de données à caractère personnel

La DPA italienne a établi des lignes directrices spécifiques afin de clarifier les obligations de notification applicables aux fournisseurs de services Internet et de télécommunications en cas de violations de données à caractère personnel. Ces lignes directrices clarifient l'identité des personnes tenues de notifier une violation et dans quelles circonstances, la nécessité ou non de notifier les utilisateurs et les parties contractantes ainsi que la manière de le faire, et quelles mesures de sécurité techniques et organisationnelles doivent être mises en œuvre (cf. la décision du 26 juillet 2012 publiée au Journal Officiel italien n° 183 du 7 août 2012 – Document Internet n° 1915485).

Forums, blogs, archives en ligne de journaux quotidiens

Les lignes directrices pour le traitement loyal des données à caractère personnel par les blogs, forums, réseaux sociaux et sites web axés sur la santé ont été publiées en février 2012. Ces lignes directrices ne s'appliquent pas aux services de santé en ligne ou de télémédecine. Les principales recommandations s'adressent aux propriétaires de sites Internet qui devront informer les utilisateurs des risques pouvant découler de la publication et de la diffusion en ligne d'informations liées à leur santé ; à cette fin, une « notification de risque » ad hoc devra être affichée sur leur page d'accueil.

Outre une décision de la Cour de cassation italienne (n° 5525/2012) sur le « droit à l'oubli », la DPA italienne a fait suite à une plainte concernant la mise à jour d'une information postée sur le site web d'un grand quotidien afin qu'il tienne compte des développements de la situation. Il convient de noter que l'article spécifique avait déjà été désindexé. Il a néanmoins été imposé à l'éditeur de signaler (par exemple, en publiant un avis à côté de l'information individuelle) une évolution ultérieure des informations publiées. Ce faisant, il s'assure que l'identité de la personne concernée est respectée tout en permettant aux lecteurs d'être informés de manière fiable et précise.

Autorisations : données génétiques et recherche médicale, biomédicale ou épidémiologique

L'autorisation générale accordée par la DPA de traiter des données génétiques a été précisée en décembre 2012 afin de tenir compte d'un avis rendu par le ministère de la Santé italien ainsi que de l'expérience accumulée et des contributions des experts faisant autorité en la matière ; elle a par ailleurs été accordée aux organisations de médiation publiques et privées conformément à la législation applicable.

L'autorisation générale accordée provisoirement en mars 2012 afin de permettre le traitement de données à caractère personnel à des fins de recherche médicale, biomédicale et épidémiologique, dans des circonstances spécifiques, sans en informer les personnes concernées, a été remaniée et étendue en décembre 2012. L'autorisation prévoit désormais que les donnés médicales puissent être traitées avec les informations relatives à la vie sexuelle, aux origines raciales ou ethniques sans le consentement des patients s'il est manifestement impossible d'informer les patients du traitement pour des « motifs éthiques » ou en raison « d'empêchements organisationnels » ; les autres conditions à remplir dans ces cas comprennent l'avis favorable et raisonné rendu sur le projet de recherche en question par le comité d'éthique compétent. Pour rappel, le consentement des patients reste nécessaire et doit être obtenu immédiatement lorsqu'ils contactent l'établissement médical en question (en particulier s'ils visitent les services ambulatoires par la suite).

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 (GTSIVP) 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) et contribue régulièrement et participe au Groupe de Berlin (groupe de travail international sur la protection des données dans les télécommunications).

La DPA a poursuivi son travail sur les projets IPA, TAIEX et de jumelage de la Commission européenne pour les nouveaux pays de l'UE, les pays candidats (Turquie, Croatie, ARYM), les pays des Balkans, la Russie et les pays adhérant à la politique européenne de voisinage afin de faciliter l'approximation de la législation dans ces pays au cadre européen de protection des données.

Organisation	Autorité italienne de protection des données
Président et/ou collège	Président du collège : Dr Antonello SORO Collège : Augusta IANNINI Giovanna BIANCHI CLERICI Licia CALIFANO
Budget	Environ 8,8 millions d'EUR (financés par le gouvernement)
Personnel	122
Activités générales	
Décisions, avis, recommandations	Nombre de décisions prises par le Collège : 440
Notifications	1 053
Examens préalables	13
Demandes émanant des personnes concernées	Nombre total de demandes : environ 4 900 Demandes d'informations (« quesiti ») : 320 Dénonciations et réclamations (« segnalazioni » et « reclami ») reçues en 2012, émanant des personnes concernées : 4 592
Plaintes émanant des personnes concernées	(plaintes officielles, réglementées spécifiquement par le Code de protection des données, concernant l'accès à ses propres données personnelles) : 233
Conseils sollicités par le	Avis rendus en réponse à des demandes du Parlement : 6

Parlement ou le gouvernement	Avis rendus aux ministères et au cabinet du Premier ministre : 23 Sujets : police, sécurité publique : 3 activité judiciaire : 2 administration en ligne et bases de données : 6 éducation et formation : 1 santé : 1 entreprises : 1 exercice des droits : 2 aides sociales : 3 documents électroniques : 2
Autres renseignements relatifs aux activités générales	Les services de première ligne de la DPA ont reçu, en 2012, environ 34 000 appels téléphoniques et courriels Autorisations nationales de transferts internationaux : 3
Activités d'inspection	
Contrôles, enquêtes	Nombre de contrôles et/ou d'enquêtes (sur place) : 395 (dont 56 infractions à caractère criminel rapportées aux autorités judiciaires)
Activités de sanction	
Sanctions	Environ 600
Amendes	Montant : environ 3,8 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 de cassation — Droit à l'oubli et mise à jour des informations

Une décision de la Cour de cassation (n° 5525/2012) concernant une information disponible en ligne dans les archives d'un célèbre quotidien a jugé que l'éditeur devait s'assurer que l'information donnée était à la fois mise dans le contexte approprié et mise à jour ; cette décision visait à protéger la personne concernée tout en fournissant au public des informations précises et approfondies. Par conséquent, la Cour a ordonné à l'éditeur de prendre des arrangements afin que l'évolution de ce cas spécifique (comme le fait qu'une décision de justice définitive ait été rendue en l'espèce) puisse être signalée aux côtés de l'article d'origine et que ces informations supplémentaires soient rendues facilement et rapidement accessibles aux utilisateurs.

Tribunal de Milan – Champ d'application géographique du code de protection des données

Statuant sur le pourvoi formé contre une décision de la DPA du 7 avril 2011, le tribunal de Milan a traité le concept « d'équipement » visé à la section 5, paragraphe 2, du code de protection des données. En particulier, le tribunal a jugé que le concept de « simple acheminement de communications » ne s'appliquait pas aux services fournis par une société de marketing qui gérait ses activités de messagerie publicitaire via des serveurs situés aux États-Unis mais acheminait une partie des télécopies destinées à l'Italie vers un nœud de livraison situé en Italie et géré par une société téléphonique établie en Italie. Ce nœud de livraison était un établissement informatique complexe qui adressait à l'expéditeur un message sur la livraison réussie ou non de chaque télécopie ; ces messages comprenaient l'adresse IP et le numéro de fax de l'expéditeur, le numéro de fax du destinataire, le résultat, le nombre de télécopies envoyées et le contenu du ou des messages envoyés. Ainsi, le système en question associait Internet au réseau téléphonique sur le territoire italien via un appareil spécifique appelé « serveur de fax », qui fonctionnait en traitant des données à caractère personnel. Compte tenu de ce qui précède, le tribunal de Milan a confirmé la décision de la DPA et jugé que les opérations de traitement en question entraient dans le champ d'application du code de protection des données italien.

Cour de cassation – Affichage d'avis publics par une municipalité

La Cour de cassation (par sa décision n° 12726/2012) a confirmé une décision de la DPA du 9 décembre 2003 traitant de l'apparition du nom d'un employé sur un avis public de convocation du conseil municipal. L'affichage public de cet avis, qui avait trait à des procédures d'exécution prises à l'encontre de l'employé, a été jugé conforme à la législation applicable sur les autorités locales (décret législatif n° 267/2000). Toutefois, la quantité d'informations personnelles dévoilées a été jugée excessive et disproportionnée en comparaison de l'objectif de transparence et d'information visé par la municipalité.

C. Autres informations importantes

Manifestations d'intérêt concernant l'apparition de l'État italien dans les procédures devant la Cour de justice de l'UE

La DPA a manifesté son intérêt pour que l'État italien se présente devant la Cour de justice de l'UE dans les affaires suivantes :

- Affaire C-119/12 (demande de décision préjudicielle au titre de l'article 267 TFUE) portant sur l'interprétation de l'article 6 de la directive 2002/58/CE, afin de soutenir une interprétation dudit article qui soit conforme à la manière dont il a été transposé dans le droit italien (cf. section 123 du code de protection des données). La disposition en question spécifie les conditions dans lesquelles les données à caractère personnel relatives au trafic peuvent être traitées à des fins commerciales (ici, la facturation) conformément aux principes de minimisation des données et de proportionnalité et en maintenant un équilibre approprié entre les différents intérêts en question.
- Affaire C-131/12 (demande de décision préjudicielle au titre de l'article 267 TFUE) portant sur l'interprétation des articles 2, 4, 12 et 14 de la directive 95/46/CE concernant, notamment, les notions d'établissement sur le territoire d'un État membre et du « recours à des moyens situés sur le territoire dudit État membre », ainsi que sur le stockage des informations indexées par les moteurs de recherche et le droit à l'effacement des données. Il a été entendu que des affaires similaires à celle qui avait vu l'Audiencia Nacional espagnole saisir la Cour de justice de l'UE avaient été traitées par la DPA, qui avait demandé aux sites sources (c'est-à-dire, aux responsables du traitement des données qui avaient été publiées puis collectées par des moteurs de recherche) de mettre en œuvre des mesures visant à empêcher les moteurs de recherche externes d'extraire les données à caractère

personnel des personnes concernées. Ces mesures comprennent, notamment, la compilation du fichier robots.txt en vertu du « protocole d'exclusion des robots » et l'emploi de « méta-tags robots ».

LETTONIE

A. Résumé des activités et actualités :

Au cours de l'année 2012, des amendements de la loi sur la protection des données à caractère personnel ont été élaborés. Ces amendements ont principalement trait aux questions suivantes :

- Clarification de la définition de responsable du traitement, y compris de la définition de responsable conjoint du traitement, déterminant les droits et devoirs et la responsabilité partagée ;
- Détermination de plusieurs exemptions de notification supplémentaires ;
- Spécification des exigences relatives aux transferts de données vers des pays tiers qui n'assurent pas le même niveau de protection des données qu'en Lettonie ;
- Exigence faite aux institutions publiques nationales ou locales de mettre en œuvre une évaluation de l'efficacité de la protection des données à caractère personnel ;
- Détermination des droits de l'Inspection nationale des données à déterminer un certain délai dans lequel les informations devraient lui être soumises de manière à ce qu'elle puisse exercer ses fonctions.

Des amendements ont par ailleurs été élaborés quant au système d'information Schengen. L'Inspection nationale des données de Lettonie, en coopération avec le ministère de la Justice, a formulé un avis selon lequel il conviendrait de réévaluer et de reconsidérer la question de savoir si toutes les institutions ont besoin d'avoir accès au SIS, et pour quelles raisons.

Au niveau national, l'Inspection nationale des données de Lettonie a exprimé son avis sur différents actes juridiques et initiatives politiques, dont les principaux sont énumérés ci-dessous :

1) Projet de loi sur le bureau des crédits ;
2) Projet de loi sur le recouvrement de créances ;
3) Projet de loi sur l'identification électronique.

En octobre 2012, la Lettonie a fait l'objet du processus d'évaluation de Schengen concernant la protection des données et ce sujet est par conséquent devenu la priorité du bureau (plusieurs activités de contrôle ont été déployées et des documents d'information ont été élaborés).

Au regard des plaintes reçues en 2011 et 2012, l'Inspection nationale des données de Lettonie a identifié les problèmes suivants comme concernant une majorité des plaintes reçues :

1) Le traitement des données à caractère personnel dans le cadre du processus de recouvrement de créances ;
2) Le responsable du traitement n'a pas communiqué les informations nécessaires à la personne concernée ;
3) Publication de données à caractère personnel sur Internet.

10 séminaires ont été organisés, ainsi que trois examens pour les délégués à la protection des données. 12 personnes ont obtenu le statut de délégué à la protection des données.

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

L'Inspection publique de protection des données n'a aucune statistique disponible sur les demandes de conseils adressées par les pouvoirs publics. Néanmoins, elle reçoit quotidiennement des appels de

différentes autorités publiques sur diverses questions liées au traitement des données à caractère personnel (à commencer par la nécessité de notifier le traitement de données à caractère personnel, les droits d'accès de la personne concernée et autres questions plus compliquées qui requièrent une analyse approfondie pour identifier la meilleure solution concernant la protection des données à caractère personnel ; par exemple, de nombreuses questions ont été soulevées par les secteurs public et privé concernant les aspects liés au traitement de données dans le cadre des relations de travail et des questions de sécurité des données, et c'est pourquoi l'Inspection nationale des données de Lettonie élaborera des recommandations sur ces questions en 2013).

Informations sur les activités de sensibilisation

L'Inspection nationale des données a organisé plusieurs séminaires sur des questions liées à la protection des données à caractère personnel, destinés à différents publics cibles tels que les établissements d'enseignement, les institutions publiques locales, les banques et les représentants du secteur financier, le personnel médical, etc. L'Inspection nationale des données propose des séminaires ouverts à toutes les personnes intéressées.

Au moins quatre demandes des médias portent chaque semaine sur différentes questions de protection des données. Les médias ont également porté leur attention sur les questions abordées par le groupe de travail « Article 29 », ainsi que sur le résultat des investigations conjointes des pays baltes sur le traitement des données à caractère personnel.

Plusieurs activités de contrôle ayant porté sur les cartes de fidélité, cette question a bénéficié du soutien des médias qui ont encouragé les gens à penser à leurs données à caractère personnel en termes de valeur et à évaluer de manière plus attentive les situations dans lesquelles ils ne doivent pas communiquer leurs données à caractère personnel aux personnes / sociétés qui leur en font la demande.

Organisation	Inspection nationale des données de Lettonie (Datu valsts inspekcija)
Président et/ou collège	Directeur — Signe Plūmiņa
Budget 2012	266 907 LVL (environ 370 457 EUR)
Personnel	19 (y compris le personnel administratif et de maintenance)
Activités générales	
Décisions, avis, recommandations	Concernant les statistiques sur les décisions et avis : s. o. Concernant les recommandations : aucune recommandation élaborée en 2012 ; deux recommandations prévues en 2013
Notifications	352 (dont les notifications sur des amendements relatifs au traitement des données à caractère personnel)
Examens préalables	234 ; axés sur les domaines à risque (déterminés pour chaque année) tels que le traitement des données sensibles, le traitement des données biométriques (vidéosurveillance incluse) et le transfert de données à caractère personnel vers des pays tiers.

Demandes émanant des personnes concernées	s. o.
Plaintes émanant des personnes concernées	Nombre total d'enquêtes : 496 (80 % des enquêtes ont été réalisées suite à des plaintes reçues). 4 plaintes émanant de personnes concernées de pays tiers concernant le traitement de leurs données à caractère personnel dans le cadre du SIS. 11 plaintes concernant les pourriels (11 enquêtes réalisées à ce sujet).
Conseils sollicités par le Parlement ou le gouvernement	Concernant plusieurs actes juridiques, tels que le projet de loi sur le bureau des crédits, le projet de loi sur le recouvrement de créances, ou encore, les amendements apportés à la loi d'exécution du Système d'information Schengen.
Autres renseignements relatifs aux activités générales	Lors des consultations téléphoniques, les principales questions posées par les appelants étaient les suivantes : 1. Certaines informations sont-elles considérées comme des données à caractère personnel ? 2. Qui peut exercer une vidéosurveillance, quand et où ? 3. Comment lutter contre le traitement illicite de données à caractère personnel sur Internet ? 4. Le traitement des données à caractère personnel dans le cadre du processus de recouvrement de créances. 5. De quelle manière les personnes concernées peuvent-elles exercer leur droit à la protection des données plus efficacement ?
Activités d'inspection	
Contrôles, enquêtes	La plupart des personnes qui ont contacté l'Inspection nationale des données de Lettonie ont indiqué une possible violation de la loi sur la protection des données à caractère personnel dans les domaines suivants (similaires à l'année précédente) : 1) traitement de données à caractère personnel sur Internet (également dans les cas où le responsable du traitement n'a pas prévu les moyens techniques appropriés pour assurer la protection des données) ; 2) traitement de données à caractère personnel lié au recouvrement de créances et à l'établissement des antécédents de crédit ; 3) vol d'identité, lorsque des données à caractère personnel sont communiquées et font, par conséquent, l'objet d'un traitement illicite (nombre de ces cas concernent la communication de données à caractère personnel erronées à la police nationale ou locale dans le cadre de plusieurs infractions administratives) ;

	4) traitement de données par des sociétés de maintenance interne ; 5) vidéosurveillance.
Activités de sanction	
Sanctions	Les sanctions de l'Inspection nationale des données sont prévues par le code letton des infractions administratives.
Amendes	Des amendes ont été imposées à hauteur de 18 910 LVL (environ 26 119 EUR). L'amende la plus élevée, d'un montant de 2 000 LVL (environ 2 762 EUR), a été imposée à une société de recouvrement de créances pour le traitement illégal de données à caractère personnel et l'absence d'information à la personne concernée. Deux amendes ont été imposées concernant le traitement de données à caractère personnel dans le cadre du SIS.
DPD	
Chiffres relatifs aux DPD	12 délégués à la protection des données enregistrés.

B. Informations sur la jurisprudence

En 2012, le nombre de cas de violation de la loi sur la protection des données à caractère personnel a augmenté et les sanctions pour de telles violations sont prévues par le droit pénal, c'est pourquoi ces affaires ont été transmises au bureau du procureur général. Le nombre de cas où il a été nécessaire de coopérer avec les DPA d'autres pays européens pour réaliser l'enquête a également augmenté.

LITUANIE

A : Résumé des activités et actualités

La Journée européenne de la protection des données a été célébrée le 30 janvier 2012. Une conférence de presse et des activités ont été organisées au Seimas de la République de Lituanie sur le sujet de la Journée de la protection des données : « Protection des données et technologies modernes ». Le 7 février 2012, la Journée européenne de la protection des données a été célébrée au lycée de Vilnius. Cette journée avait pour objectif une meilleure compréhension des menaces pesant sur la sécurité des données à caractère personnel dans le cadre de l'utilisation des technologies modernes. Le principal groupe cible était celui des élèves du lycée, ainsi que le grand public.

En mars 2012, les autorités de contrôle de la protection des données estonienne, lettone et lituanienne se sont réunies en Estonie dans l'objectif d'inaugurer la coopération des États baltes. Lors de cette réunion, il a été décidé de réaliser des enquêtes conjointes au sein de sociétés internationales déployant des activités dans ces trois pays. Des informations sur les principales activités prévues et les priorités des établissements pour 2012 ont été échangées et les principales questions liées à la future évaluation de Schengen et de la réforme de la protection des données européenne ont été discutées. Une décision a également été prise d'organiser des réunions de ce genre chaque année.

Suite à cette réunion de 2012, des enquêtes conjointes ont été réalisées dans les hôtels appartenant au réseau international Radisson Blue des trois pays. Ces enquêtes avaient pour but de contrôler la légalité du traitement des données à caractère personnel des clients des hôtels dans le cadre de leur hébergement. Lors de ces enquêtes, plusieurs incompatibilités avec les exigences de protection des données à caractère personnel ont été établies et des ordonnances ont été adressées aux hôtels.

Le 19 mai 2012, l'IPPD et la société par actions Expozona ont organisé une conférence intitulée « Le traitement des données à caractère personnel des employés et la divulgation de données à des tierces parties — thématiques et problèmes ». L'événement était dédié au 15e anniversaire de l'IPPD et consacré aux sociétés, établissements et organisations, responsables, avocats et professionnels responsables du traitement des données à caractère personnel des employés.

Le 14 juin 2012, la confédération lituanienne des entreprises et l'IPPD ont signé un accord de coopération dans le but d'obtenir une coopération plus efficace et constructive entre les entreprises et les établissements publics dans le domaine de la protection des données à caractère personnel. Cette coopération renforcée contribuera à prévenir les violations de la loi sur la protection juridique des données à caractère personnel de la République de Lituanie (ci-après, la LPJDP) et à encourager la communauté des entreprises à respecter les règles de protection des données à caractère personnel.

Organisation	Inspection nationale de protection des données
Président et/ou collège	Dr Algirdas Kunčinas
Budget	Alloué et exécuté : 2 001 millions de LTL (579 530 EUR)
Personnel	30
Activités générales	
Avis, recommandations	s. o.

Notifications	1 258
Examens préalables	308
Demandes émanant des personnes concernées	15
Plaintes émanant des personnes concernées	324
Conseils sollicités par le Parlement ou le gouvernement	s. o.
Autres renseignements relatifs aux activités générales	4 008 consultations ; 103 communiqués d'information au public ; 3 synthèses des résultats des enquêtes préventives et de la jurisprudence ; 99 conclusions sur les documents de l'UE et du Conseil de l'Europe ; 108 réponses à des demandes de parties à la Convention (STE n° 108) ; 277 actes juridiques coordonnés et documents des responsables du traitement des données ; 6 actes juridiques préparés et 4 consultations publiques.
Activités d'inspection	
Contrôles	45 (portée et légitimité du traitement des données, et droits des personnes concernées dans les boutiques en ligne, entreprises de services publics).
Activités de sanction	
Sanctions	L'IPPD a mis en place 37 protocoles pour des infractions administratives.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Traitement de données à caractère personnel de responsables d'entités juridiques

L'IPPD a reçu une plainte questionnant les fondements juridiques dont disposait l'association pour communiquer des informations à des journalistes sur les dettes du plaignant auprès d'associations, qui avaient été publiées dans le journal. L'IPPD a conclu que, dans le journal, toutes les données faisaient exclusivement référence au plaignant en tant que responsable de la société et que la LPJDP n'était dès lors pas applicable. Cette décision a fait l'objet d'un appel de la part du plaignant devant le tribunal administratif de grande instance de Vilnius. Le tribunal a rejeté l'appel comme étant non fondé, concluant que les données sur la société, telles que le nom de son responsable, devaient être considérées comme étant les données d'une entité juridique. Le plaignant a fait appel de cette décision devant la Cour administrative suprême, qui a également statué que ces données devaient être considérées comme les

données d'une entité juridique, qui sont à la disposition du public et librement disponibles pour toute personne, et que la LPJDP, qui réglemente le traitement des informations liées à une personne physique, n'avait dès lors pas été enfreinte.

Publication de données à caractère personnel sur Internet à des fins préventives

L'IPPD a élaboré un protocole applicable aux infractions administratives d'une entreprise forestière (ci-après « l'entreprise »), qui publiait sur son site Internet des données à caractère personnel (nom, prénom, adresse résidentielle complète et informations sur le protocole d'infraction administrative adressé à la personne, mais pas encore applicable) sans aucun fondement juridique en vertu de l'article 5 de la LPJDP ou tout autre critère de publication licite des données mentionnées. Le tribunal de grande instance a fermé cette affaire d'infraction administrative sans avoir jugé que l'entreprise était coupable. Le tribunal a conclu que les données mentionnées étaient publiées dans un intérêt légitime de prévention, sachant que l'article 254 du Code administratif de la République de Lituanie prévoit que les cas d'infractions administratives soient rendus publics. Dans l'objectif d'optimiser le rôle éducatif et préventif de ces affaires, celles-ci peuvent être entendues directement au niveau des collectifs de travailleurs, du lieu d'apprentissage ou de résidence de la personne responsable sur le plan administratif.

Sur demande de l'IPPD, la Cour administrative suprême a rouvert le processus et établi que, dans ce cas, la divulgation de données à caractère personnel constituait une violation de la LPJDP. La cour a reconnu que la prévention des délits administratifs était l'un des motifs légitimes possibles du traitement de données à caractère personnel. Néanmoins, après avoir évalué et pesé l'objet de la publication et la nature et l'exhaustivité des données à caractère personnel publiées, ainsi que le fait que des informations aient été publiées sur des protocoles non encore applicables et aient continué à être publiées malgré le fait que la personne ait fait appel du protocole en question, un groupe de juges a décidé que, dans ce cas, l'intérêt public de la prévention des infractions n'était pas supérieur au droit à la vie privée d'une personne. La Cour administrative suprême a décidé que, dans ces circonstances, la fonction préventive et éducative pouvait être exercée sans divulguer des données à caractère personnel aussi détaillées (nom, prénom et adresse de résidence), d'autant plus que le lieu de résidence n'est généralement pas associé au délit administratif et n'a aucun effet éducatif, ce qui rend la publication de l'adresse excessive. La publication des nom et prénom de la personne n'a d'effet que sur la personne concernée. Pour le grand public, l'impact préventif et éducatif découle des informations qui indiquent le caractère inévitable de la responsabilité, le fait que le délit est condamnable et les sanctions appliquées à la personne.

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 2012.

Principales questions abordées

La CNPD a conseillé le gouvernement du Luxembourg en donnant son avis sur un vaste éventail de lois et règlements pour lesquels elle a été consultée. Les principales questions abordées en 2012 ont été les suivantes :

- la mise en œuvre d'une base de données nationale des élèves par le ministère de l'Éducation ;
- le registre national des personnes physiques, les registres municipaux de la population et la carte d'identité électronique ;
- le registre national du cancer ;
- la réforme de la loi concernant les casiers judiciaires ;
- la loi sur le surendettement ;
- l'introduction d'un système de pétition électronique pour le Parlement du Luxembourg.

Actualités

En 2012, la DPA luxembourgeoise a dû intervenir plusieurs fois pour contrôler le respect de la loi sur la protection des données. En une occasion, une intrusion dans une base de données du ministère des Sports contenant les informations personnelles de plus de 48 000 personnes a été constatée. Dans le cadre d'une autre affaire, la CNPD a vérifié si la période de conservation des photos de citoyens qui avaient été stockées avait été respectée lors du remplacement de leurs cartes d'identité défectueuses. En décembre 2012, la CNPD et la CNIL (France) ont été invitées par le groupe de travail « Article 29 » à diriger l'analyse du « contrat de services Microsoft » et de la « politique de confidentialité en ligne de Microsoft ».

Principaux événements et activités de sensibilisation

La CNPD a organisé au Luxembourg la Conférence de printemps des autorités européennes de protection des données, qui s'est tenue du 2 au 4 mai 2012. 138 commissaires de 38 pays et des représentants de la Commission européenne, du Conseil de l'Europe et de l'OCDE ont participé à la conférence sur le thème suivant : *« La réforme de la protection des données européenne confrontée aux attentes ! »*. Cet événement offrait l'occasion de discuter de la manière dont la modernisation du cadre juridique européen améliorerait le respect de la vie privée des citoyens à l'ère du numérique et dans un monde globalisé, ainsi que des mesures à prendre pour préparer ces changements.

Au-delà de ce grand événement, la DPA luxembourgeoise a participé à plusieurs événements de sensibilisation destinés au grand public, tels que la Journée européenne de la protection des données, dont le slogan était *Votre vie privée n'est pas privée de droits*. La CNPD a également participé à plusieurs séminaires et formations visant à sensibiliser un public plus spécialisé.

Organisation	Commission nationale pour la protection des données (CNPD)
Président et/ou collège	M. Gérard LOMMEL — Président M. Thierry LALLEMANG — Commissaire M. Pierre WEIMERSKIRCH — Commissaire
Budget	1 636 000 EUR
Personnel	Collège : 3 Service juridique : 5 Notifications et vérifications préalables : 2 Administration générale : 3 Communication et documentation : 1 Informatique et logistique : 1 Total : 15
Activités générales	
Décisions, avis, recommandations	438
Notifications	586
Examens préalables	423
Demandes émanant des personnes concernées	228
Plaintes émanant des personnes concernées	133
Conseils sollicités par le Parlement ou le gouvernement	6
Autres renseignements relatifs aux activités générales	Réunions et consultations (avec les secteurs public/privé) : 132 Conférences et réunions d'information : 10 Cas de règles d'entreprise contraignantes où la DPA est l'autorité « chef de file » : 2
Activités d'inspection	
Contrôles, enquêtes	18
Activités de sanction	
Sanctions	0

Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	DPD désignés en 2012 : 11 Nombre total de DPD désignés (à la date du rapport) : 47

B. Informations sur la jurisprudence

13e chambre correctionnelle du tribunal d'arrondissement de Luxembourg (1er février 2012, n° 534/2012) sur la validité de preuves (images de vidéosurveillance) collectées en l'absence d'autorisation préalable de la CNPD.

Cette affaire portait sur un accident avec délit de fuite dans un tunnel, enregistré par des caméras de vidéosurveillance pour lesquelles aucune autorisation préalable n'avait été demandée. L'avocat de la défense a plaidé *« in limine litis »* que les bandes vidéo de l'accident ne pouvaient être utilisées comme preuves, étant donné qu'aucune autorisation préalable de la CNPD n'avait été obtenue.

Le tribunal a jugé que les images devaient néanmoins être autorisées comme moyens de preuve. Pour conclure de cette manière, le tribunal a analysé les conditions de légitimité de ladite surveillance et a clairement fait référence au critère de l'objectif défini par la loi luxembourgeoise sur la protection des données.

Contrairement à l'affaire rapportée en 2009 (9e chambre correctionnelle du tribunal d'arrondissement de Luxembourg, n° 387/2009) et que la CNPD avait jugée hautement préjudiciable, dans la mesure où elle reposait sur de vagues concepts judiciaires et la conviction intime du juge, cette nouvelle affaire introduit une manière plus transparente et correcte d'analyser la validité de la preuve en l'absence d'autorisation préalable de la CNPD.

MALTE

A : Résumé des activités et actualités :

Au cours de l'année de référence, la loi sur la protection des données n'a fait l'objet d'aucune intervention législative. Une notification juridique établissant le 1er janvier 2013 comme la date à laquelle l'ensemble des dispositions de la notification juridique 239 de 2011 devaient entrer en vigueur était néanmoins en cours d'élaboration. Ce règlement transpose la directive « Vie privée et communications électroniques » 2009/136/CE amendée du Parlement européen et du Conseil du 25 novembre 2009, qui modifie, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Notre Bureau a initié le processus de développement de lignes directrices ad hoc afin de fournir aux responsables du traitement de données les instructions nécessaires concernant la mise en œuvre de l'exigence de consentement pour les cookies.

La loi sur la liberté d'information (chapitre 496 des lois maltaises) a été adoptée par le Parlement en 2008. La loi a pour objet d'établir le droit à l'information des autorités publiques afin de promouvoir une transparence et une responsabilité accrues du gouvernement. La loi est entrée pleinement en vigueur le 1er septembre 2012 et confère au Commissaire de nouvelles responsabilités et, notamment, celles de recevoir et de décider quelles décisions devront être examinées par les autorités publiques, d'adresser des avis d'exécution aux autorités publiques afin de faire respecter ses décisions et de promouvoir le respect de la loi. Pendant la période concernée, le Commissaire a reçu trois plaintes, dont deux à l'encontre des forces de police maltaises et une à l'encontre du secrétariat permanent du ministère des Affaires intérieures.

Notre bureau a maintenu ses efforts pour rencontrer les différents secteurs dans l'objectif de discuter des questions de protection des données et d'apporter les conseils nécessaires. Des réunions ont été organisées avec les deux principales agences de notation de crédit de l'île et, après une série de discussions, des lignes directrices ont été formulées et adoptées afin de promouvoir de bonnes pratiques dans le domaine du traitement des données à caractère personnel par les établissements de crédit.

En 2012, quatre personnes se sont senties lésées par la décision du Commissaire et ont fait appel devant la Cour d'appel pour la protection des données et de l'information. Si un appel a été retiré par la partie appelante suite à la première audience du Tribunal, les poursuites liées au second appel étaient toujours en cours en fin d'année et, dans les deux autres affaires, le président du tribunal s'est prononcé en faveur du Commissaire et a rejeté les appels. Ces décisions ont été considérées comme définitives et probantes étant donné qu'aucune des parties n'a fait appel de ces décisions devant la Cour d'appel dans le délai de trente jours alloué par la loi.

Suite à la première évaluation du comité d'évaluation Schengen de la protection des données en 2006, dans le cadre des préparations de Malte à l'accession à l'espace Schengen, notre bureau a fait l'objet d'un deuxième examen par des pairs de la part du même comité d'évaluation en juillet. Des experts ont appelé le bureau afin d'évaluer les opérations et procédures internes et, en particulier, l'exercice du rôle de supervision du Commissaire. Des présentations ont été réalisées par le Commissaire, le personnel technique et le responsable de la protection des données au sein du ministère des Affaires étrangères. Le résultat de l'évaluation a été présenté au groupe de travail Schengen lors de la réunion du Conseil, où il a été conclu que notre bureau était prêt à exercer le rôle de régulateur de la protection des données auprès de tous les responsables du traitement des données, police comprise. Un nombre minimal de recommandations a également été formulé, et notre bureau a immédiatement pris des mesures pour y répondre.

Le 28 janvier, notre bureau a rejoint les autres autorités de protection des données européennes afin de célébrer la Journée européenne de la protection des données. Pour marquer cet événement sur le plan

local, notre bureau a distribué des documents d'information et du matériel de papeterie aux élèves de toutes les écoles publiques et privées. Notre bureau a toujours été fermement convaincu que, si l'on souhaite que la culture évolue de manière efficace, des investissements continus doivent être consacrés à l'éducation et à la sensibilisation des jeunes générations.

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

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	Environ 300 000 EUR
Personnel	Commissaire – 1 Personnel spécialisé – 3 Assistance technique – 2 Assistance administrative – 3
Activités générales	
Décisions, avis, recommandations	48 décisions ont été émises dans le cadre de plaintes reçues par le commissaire 23 avis/recommandations ont été émis relativement à des avis publiés sous forme d'articles de journaux ciblant à la fois le grand public et les responsables du traitement des données, et d'autres avis/recommandations ont été adressés aux responsables du traitement sur des sujets spécifiques.
Notifications	228 nouvelles notifications ont été reçues
Examens préalables	5 demandes d'examens préalables ont été reçues
Demandes émanant des personnes concernées	Demandes reçues par téléphone – 10 appels quotidiens en moyenne Demandes reçues par courriel – 156
Plaintes émanant des personnes concernées	72 plaintes

Conseils sollicités par le Parlement ou le gouvernement	s. o.
Autres renseignements relatifs aux activités générales	s. o.
Activités d'inspection	
Contrôles, enquêtes	8 contrôles ont été réalisés dans le cadre d'enquêtes sur des plaintes reçues de la part de personnes concernées et d'enquêtes de routine sur les systèmes de police et, notamment, le SIS et Europol.
Activités de sanction	
Sanctions	Des réprimandes officielles ont été adressées à des responsables du traitement de données. Aucune procédure judiciaire n'a été initiée devant les tribunaux.
Amendes	Aucune amende financière n'a été imposée à des responsables du traitement de données.
DPD	
Chiffres relatifs aux DPD	12 représentants des données personnelles ont été désignés.

B. Informations sur la jurisprudence

Aucune jurisprudence n'est disponible pour la période examinée.

PAYS-BAS

A : Résumé des activités et actualités :

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

Les priorités sont déterminées sur la base d'une évaluation continue des risques pour laquelle nous utilisons les signaux que nous recevons de la part de différentes sources de la société via divers canaux tels que des appels téléphoniques, des courriels et des articles de presse, etc. En 2011, un nouveau système d'enregistrement des signaux a été introduit, qui nous permet d'enregistrer les signaux par secteur. L'évaluation des risques tient compte de la gravité de l'infraction présumée, du nombre de personnes 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 à grande échelle de nouvelles technologies. En 2012, la DPA néerlandaise s'est essentiellement focalisée sur les éléments suivants : le profilage, la protection adéquate des données médicales et la sécurité des données.

L'une des principales enquêtes réalisées en 2012 portait sur les activités de profilage d'une grande chaîne de supermarchés aux Pays-Bas. Les déclarations publiques du détaillant ont révélé son intention de proposer à ses clients des offres personnalisées fondées sur l'analyse de leurs achats. À ces fins, la chaîne de supermarchés devait utiliser les informations collectées à partir de tous les achats effectués en utilisant la carte de fidélité des clients. Suite à son enquête, la DPA néerlandaise a conclu que le consentement demandé par le détaillant à ses clients était invalide, en raison, notamment, de l'absence d'information sur la collecte de données et les analyses subséquentes. Faisant suite à cette conclusion, le détaillant a décidé de repousser le lancement de son programme d'offres personnalisées. D'un autre côté, il a mis à jour sa politique de confidentialité et ses conditions générales, en vertu desquelles il redemandera le consentement de ses clients.

Une autre enquête réalisée en 2012 a fait suite aux protestations publiques relatives à une émission télévisée qui souhaitait montrer le fonctionnement du service des urgences d'un grand hôpital d'Amsterdam. Pour ce programme, des patients et membres du personnel étaient filmés le temps de leur passage par le service. Si l'équipe de télévision évaluait le « cas » d'un patient suffisamment intéressant pour être diffusé, son autorisation lui était demandée d'utiliser les images pour les diffuser et d'en enregistrer de nouvelles. Compte tenu de la nature du lieu des enregistrements (un hôpital), ces derniers devaient contenir principalement des informations médicales requérant une attention particulière. La DPA néerlandaise a conclu pour diverses raisons que le consentement requis n'avait pas été obtenu légalement par l'équipe de télévision. En premier lieu, le consentement n'avait pas été obtenu avant le début du traitement des données, puisque les images étaient enregistrées depuis l'arrivée des patients et de l'équipe au service d'urgence. En outre, les informations fournies étaient insuffisantes pour que les patients puissent prendre une décision éclairée. Enfin, étant donné que les patients entrant au service d'urgence sont en général dans une situation de détresse, leur dépendance vis-à-vis des services de l'hôpital est telle que, d'après la DPA néerlandaise, leur consentement, même éclairé, ne pouvait être considéré comme ayant été donné librement.

Outre la réalisation de ces enquêtes, la DPA néerlandaise offre au gouvernement ses conseils sur les projets de loi avant qu'ils ne soient envoyés au Parlement. Grâce à ces conseils de la DPA, des propositions sont (parfois) amendées afin d'éviter des violations de la vie privée. En 2012, des conseils ont été donnés quant à une proposition visant à autoriser une nouvelle augmentation des loyers de foyers ayant des revenus moyens (compris entre 33 000 EUR et 43 000 EUR par an). Une augmentation annuelle du loyer correspondant à l'inflation plus un pour cent devait être appliquée à ces locataires. Afin d'évaluer quels locataires pouvaient faire l'objet de cette augmentation, les autorités fiscales devaient transférer les informations sur la catégorie de revenus des locataires aux propriétaires. La DPA

néerlandaise a jugé que la proposition n'était pas suffisamment motivée et ne respectait pas les exigences de proportionnalité et de subsidiarité. Le Gouvernement n'avait pas démontré dans quelle mesure cette violation du droit fondamental à la protection des données contribuerait à améliorer la disponibilité des propriétés à louer (l'objet identifié du projet de loi) et la raison pour laquelle une alternative moins intrusive ne pouvait être utilisée pour un résultat similaire.

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 : 7 679 000 EUR Exécuté : 7 746 000 EUR
Personnel	75,8 ETP
Activités générales	
Décisions, avis, recommandations	213 (enquêtes, lignes directrices, code de conduite, examens préalables, sanctions et conseils dans le cadre du processus législatif)
Notifications	5 966
Examens préalables	93
Signaux ([12]) émanant des personnes concernées	6 042
Conseils sollicités par le Parlement ou le gouvernement	42
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	58

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

Activités de sanction	
Sanctions	12
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	345 ([13])

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. Dans l'une de ces affaires, notamment, le tribunal d'Amsterdam a jugé qu'un livre pouvait être considéré comme un fichier dans le sens de la législation sur la protection des données si un registre de personnes y est inclus. Dans une affaire liée au montant de loyers dus pour certains types de logements, la cour de La Haye a décidé que la loi néerlandaise sur la protection des données devait être lue dans son intégralité en conjonction avec l'article 8 de la CEDH sur le droit à la vie privée. La proportionnalité et la subsidiarité doivent être prises en compte en toutes circonstances, ainsi qu'en relation avec l'objet de la mesure proposée, et ne peuvent être ignorées en vertu d'une décision ministérielle.

Dans le cadre d'une affaire traitée en 2012, une décision de la DPA néerlandaise a fait l'objet d'une procédure devant le tribunal de Rotterdam. Le quartier Charlois de la municipalité de Rotterdam avait introduit une obligation d'enregistrement du pays de naissance afin de mettre en œuvre un traitement préférentiel en matière d'assistance apportée aux enfants ayant plusieurs problèmes (retards à l'école, tendances criminelles précoces, maltraitance, etc.).[14] Considérant que la plupart des enfants ayant des problèmes ne sont pas d'origine néerlandaise, le quartier considérait utile de pouvoir trier les possibles situations problématiques en fonction du pays de naissance. La DPA néerlandaise a néanmoins jugé qu'il s'agirait en fait d'une forme de profilage racial et, donc, de traitement de données sensibles. Aucune base légale n'existant pour ce type de traitement, la DPA néerlandaise a ordonné au quartier de mettre un terme à l'enregistrement du pays de naissance et imposé une amende avec sursis de 2 000 EUR par jour de poursuite du traitement. Le quartier a fait appel de la décision, mais a perdu la procédure et a dû mettre un terme au traitement contentieux.

([13]) Nombre correct en septembre 2013.

([14]) Se reporter également au 15e Rapport annuel couvrant l'année 2011.

POLOGNE

A. Résumé des activités et actualités

La loi sur l'échange d'informations entre les autorités répressives des États membres de l'Union européenne (Journal officiel de 2011 n° 230, article 1371) est entrée en vigueur le 1er janvier 2012. Cette loi transposait partiellement 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 dans le cadre juridique polonais et a en même temps modifié certaines dispositions de la loi sur la protection des données à caractère personnel.

Conséquences de la dérogation du 1er janvier 2012 de l'article 7a (2) de la loi du 19 novembre 1999. En vertu de la loi sur les activités commerciales (Journal officiel de 1999 n° 101, article 1178), qui exclut les données à caractère personnel figurant dans les registres d'activités commerciales de l'application des dispositions de la loi du 29 août 1997 sur la protection des données à caractère personnel (Journal officiel de 2002 n° 101, article 926 et les amendements correspondants), ci-après la « loi », les données à caractère personnel des personnes physiques, qu'elles déploient des activités économiques ou non, font actuellement l'objet de la protection prévue par la loi.

En 2012, l'équipe d'exécution administrative a commencé à travailler. Cette nouvelle unité organisationnelle du Bureau du GIODO a été établie par le GIODO en raison d'un amendement de la loi sur la protection des données à caractère personnel entré en vigueur le 7 mars 2011 et octroyant à l'Inspecteur général pour la protection des données à caractère personnel (GIODO) les pouvoirs d'une autorité d'application dans le cadre de l'exécution administrative d'obligations non pécuniaires (Article 12, alinéa 3).

Les 15-17 avril 2012, la seconde mission d'évaluation a été conduite en Pologne afin d'évaluer le niveau de mise en œuvre des acquis de Schengen. Dans le rapport de mission, la CE a souligné les résultats importants obtenus par le GIODO dans les domaines de l'éducation et de l'information et a attribué une note très élevée aux outils juridiques pour la protection des données en Pologne et aux compétences du GIODO en matière de supervision et de contrôle du traitement de données à caractère personnel en Pologne.

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

1. L'Inspecteur général a participé à une réunion de la Commission de la justice et des droits de l'homme au Sejm (16 février 2012) et au Sénat (les deux chambres du Parlement polonais) où il a présenté aux membres du Parlement les objectifs de base de la réforme de la protection des données européenne.
2. Le 7 mars 2012, l'Inspecteur général pour la protection des données à caractère personnel, l'école nationale d'administration publique (KSAP) et la représentation de la Commission européenne en Pologne ont organisé au siège du KSAP à Varsovie une conférence sur la « Réforme des règles de protection des données à caractère personnel au sein de l'Union européenne : Évaluation préliminaire de son champ d'application et de ses conséquences ». La conférence a lancé une discussion exhaustive sur les plans de création d'un nouveau modèle de protection des données et de la vie privée au sein de l'Union européenne.
3. Dans le cadre de la réforme de la protection des données européenne, l'Inspecteur général participe à des consultations avec différents secteurs. Il a pour l'heure participé à des réunions de consultation avec les secteurs et établissements suivants :
   - le secteur bancaire ;

- l'association des assurances polonaises ;
- l'organisation polonaise du commerce et de la distribution ;
- les représentants du secteur des télécommunications et des technologies de l'information associés au sein de la Chambre polonaise des technologies de l'information et des télécommunications ;
- le Conseil judiciaire national ;
- et d'autres.

4. Le GIODO a participé à la réunion interparlementaire de commissions consacrée à « La réforme du cadre de la protection des données dans l'Union – Inspirer la confiance dans un monde numérique et global », qui s'est tenue les 9 et 10 octobre 2012 au Parlement européen à Bruxelles. La réunion interparlementaire de commissions, préparée conjointement par la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) et l'unité du dialogue législatif (UDL), devait permettre de mener une réflexion sur les problèmes les plus importants et d'associer les députés du Parlement européen et des parlements nationaux à un échange de vues et à un dialogue constructif.
5. La rencontre entre le GIODO et le Contrôleur européen adjoint de la protection des données a eu lieu le 12 décembre 2012, et le GIODO et les représentants des administrations publiques ont pu y discuter des questions liées à la réforme de la protection des données européenne et de son impact sur le droit national.

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	126
Activités générales	
Décisions, avis, recommandations	1 297 décisions émises (427 décisions liées aux procédures d'enregistrement, 53 en relation avec des enquêtes réalisées, 762 en conséquence de procédures initiées par une plainte et 51 concernant l'autorisation de transfert de données vers un pays tiers). 126 demandes ont été adressées aux autorités publiques, aux autorités des territoires autonomes, ainsi qu'aux unités organisationnelles d'État et municipales, et aux entités privées exécutant des tâches publiques, aux personnes physiques et morales, aux unités organisationnelles sans personnalité juridique et autres entités afin d'assurer une protection efficace des données à caractère personnel.
Notifications	16 267 fichiers de données à caractère personnel enregistrés.

Examens préalables	En conséquence des procédures d'enregistrement (examen préalable), 3 359 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. En connexion avec la mise en œuvre des composants nationaux du système VIS, des enquêtes ont été réalisées sur le système d'information national (KSI) à la préfecture de police en vertu de la loi du 24 août 2007 sur la participation de la République de Pologne au Système d'information Schengen et au système d'information sur les visas.
Demandes émanant des personnes concernées	4 208 questions juridiques ont été envoyées à la DPA polonaise. 11 001 explications ont également été fournies grâce à la ligne d'information du GIODO.
Plaintes émanant des personnes concernées	Plaintes concernant des atteintes à la protection des données à caractère personnel, notamment dans les domaines suivants : administration publique (88 plaintes) ; tribunaux, services du procureur général, police, huissiers (44 plaintes) ; banques et autres établissements financiers (129 plaintes) ; Internet (84 plaintes), marketing (28 plaintes), questions liées au logement (56 plaintes), assurances sociales, de biens et individuelles (12 plaintes) ; Système d'information Schengen (12 plaintes), télécommunications (40 plaintes), emploi (11 plaintes), autres (386 plaintes).
Conseils sollicités par le Parlement ou le gouvernement	Des avis ont été exprimés sur 598 projets de lois soumis à l'analyse du GIODO.
Autres renseignements relatifs aux activités générales	66 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. 207 établissements éducatifs, dont des écoles primaires, élémentaires et secondaires et centres de formation professionnelle destinés aux enseignants, ont participé à la 3e 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 académique 2012/2013.

Activités d'inspection	
Contrôles, enquêtes	165 contrôles, y compris : - 17 contrôles concernant le traitement de données à caractère personnel dans le système d'information national permettant aux autorités administratives publiques et aux autorités judiciaires d'utiliser des données collectées dans le SIS et le VIS ; - 9 contrôles au sein de banques coopératives et 2 au sein de banques associées à des banques coopératives ; - 5 contrôles auprès d'opérateurs de réseaux de télécommunications publics et de prestataires de services de télécommunications accessibles au public ; - 8 contrôles au sein de centres de dons de moelle osseuse ; - 10 contrôles du système d'information de l'enseignement supérieur ; - 11 contrôles au sein d'entités gérant des hôtels.
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, 99 procédures administratives ont été instituées dans le cadre de l'exécution des décisions du GIODO. En ce qui concerne les contrôles réalisés en 2012, le GIODO a initié 46 procédures administratives à l'encontre de responsables du traitement de données et prononcé 23 décisions ordonnant la restauration d'une situation légale appropriée. Le GIODO a également émis 64 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 2012.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

En 2012, parmi les affaires traitées par le GIODO, 73 jugements ont été émis par la Cour administrative suprême et le tribunal administratif de la voïvodie. Les jugements suivants ont notamment été rendus.

I. Jugement (Réf. N° II SA/WA 2333/11) rendu par le tribunal administratif de voïvodie de Varsovie

Le tribunal a confirmé le point de vue négatif du GIODO sur l'affaire en vertu de laquelle une société avait demandé à un syndicat opérant en son sein de divulguer la liste des noms de ses membres afin de vérifier les droits spécifiques des membres du conseil de ce syndicat. Le tribunal a souligné que donner le nombre de membres du syndicat serait suffisant pour effectuer cette vérification, et que la collecte de données sensibles, à savoir des données sur les adhérents au syndicat, à ces fins par l'employeur, ne reposait sur aucune base juridique au sens de l'article 27 (alinéa 1) de la loi sur la protection des données à caractère personnel, ou de dispositions spécifiques de la loi sur les syndicats ou du Code du travail. D'un autre côté, le tribunal a jugé que cette demande de divulgation de la liste des noms de tous les membres constituait une violation des principes de limitation de la finalité, de nécessité et de proportionnalité.

II. Jugement (Réf. N° II SA/WA 2367/11) rendu par le tribunal administratif de voïvodie de Varsovie

Le tribunal s'est déclaré en accord avec l'évaluation du GIODO dans l'affaire concernant le traitement de données à caractère personnel lié à la cession de créances, datant de l'époque où le plaignant déployait des activités commerciales et était directement lié à ces activités. Selon l'avis du tribunal, l'autorité de protection des données n'est pas compétente pour évaluer la correction de contrats de droit civil et les litiges en découlant et, notamment, pour évaluer si un contrat de cession de créances est admissible, effectif ou valide, dans la mesure où seuls les tribunaux ordinaires sont matériellement compétents en la matière. D'un autre côté, en vertu des principes de la protection des données à caractère personnel, la divulgation de données à caractère personnel liée à la cession de créances ne violait pas les dispositions de la loi sur la protection des données à caractère personnel.

III. Jugement (Réf. N° II SA/WA 2848/11) rendu par le tribunal administratif de voïvodie de Varsovie

Le tribunal a confirmé l'avis de la DPA, en vertu duquel la divulgation par une société de factures contenant les données à caractère personnel du plaignant au tribunal régional aux fins de poursuites civiles et à la préfecture de police aux fins de poursuites pénales trouve un fondement juridique en l'article 23, alinéa 1, points 2 et 5 de la loi sur la protection des données à caractère personnel, c'est-à-dire si elle est nécessaire, aux fins de l'exercice des droits et devoirs résultant d'une disposition juridique, et si le traitement est nécessaire à la réalisation d'intérêts légitimes poursuivis par les responsables du traitement des données. Par ailleurs, le tribunal, se référant à la jurisprudence établie par les tribunaux administratifs, a confirmé que le GIODO n'était pas compétent pour contrôler les actes de procédures de droit pénal ou civil menées par les autorités compétentes, telles que les procédures probatoires faisant appel à des données à caractère personnel.

C. Autres informations importantes

Pendant la période de référence, l'évolution à la hausse du nombre de fichiers de données à caractère personnel enregistrés par rapport aux années précédentes (en 2010 : 9 921, en 2011 : 11 845, en 2012 : 16 267) s'est confirmée. Par ailleurs, le nombre de fichiers notifiés à des fins d'enregistrement a fortement augmenté (de 40 % par rapport à 2011, de 164 % par rapport à 2010 et de 184 % par rapport à 2009). En 2012, le GIODO a traité 4 090 notifications de mise à jour soumises par des responsables du traitement de données et émis 287 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 30 janvier 2012, l'Inspecteur général a organisé une traditionnelle journée portes ouvertes pour tous les citoyens au siège de son Bureau, ainsi qu'une conférence intitulée « Que sait l'État de ses citoyens ? Principes du traitement des données dans les registres publics ». Comme à l'habitude, la Journée européenne de la protection des données a également été célébrée à Bruxelles.

Face au grand intérêt qu'a manifesté le public pour les journées portes ouvertes organisées à l'occasion de la Journée de la protection des données en janvier à son siège de Varsovie, le GIODO a entrepris une nouvelle initiative qui consiste à organiser ce genre d'événements à d'autres dates dans d'autres villes de Pologne. En 2012, d'autres journées portes ouvertes ont été organisées le 22 novembre à Dąbrowa Górnicza et le 23 novembre à Cracovie.

Les 23 et 24 avril 2012, la 51e réunion du groupe de travail international sur la protection des données dans les télécommunications (le Groupe de Berlin) a été organisée par le GIODO à Sopot, en Pologne. Cette réunion portait essentiellement sur le traitement des données dans les solutions d'informatique en nuage, l'exécution du droit à l'oubli et le profilage des internautes par les sociétés de marketing à l'aide d'outils d'analyse spéciaux. La grande réussite de la réunion a été l'adoption d'un document de travail comprenant la position commune du Groupe sur les principes de protection de la vie privée en cas de traitement des données via l'informatique en nuage, intitulé Mémorandum de Sopot.

Le projet de partenariat Leonardo da Vinci 2012, « Sensibilisation aux questions de protection des données parmi les employés travaillant au sein de l'UE », a été lancé en 2012. Ce projet vise à fournir de la documentation éducative aux personnes physiques occupant un emploi dans l'un des pays participant au projet. Les partenaires du projet, c'est-à-dire les autorités de la protection des données en Pologne, en République tchèque, en Croatie et en Bulgarie, participent aux travaux de publication qui porteront essentiellement sur la communication de conseils sur la protection des données à caractère personnel et la vie privée aux personnes physiques employées ou prévoyant d'être employées dans l'un des pays participant au projet.

Il convient en outre de noter que le « Code de bonnes pratiques en matière de protection des données à caractère personnel des clients et des prospects » a été développé par l'Association de l'industrie automobile polonaise en coopération avec le GIODO. Ce document fait partie intégrante d'un accord sur la coopération conclu entre les deux institutions le 16 novembre 2012.

PORTUGAL

A. Résumé des activités et actualités

En 2012, la DPA a consolidé ses procédures internes de dématérialisation, augmentant ainsi les possibilités de notification électronique du traitement de données et réduisant le temps de réponse aux responsables du traitement de données.

D'un autre côté, la DPA a accru ses activités d'inspection à la suite de plaintes émanant de personnes concernées ou de sa propre initiative. La vidéosurveillance, les communications électroniques non sollicitées à des fins de marketing et le contrôle des employés sur le lieu de travail (par exemple, avec l'implantation de GPS dans les véhicules) ont été les principaux sujets des plaintes reçues.

La DPA a continué de suivre de près l'évolution des projets d'administration en ligne des organismes publics, notamment dans le secteur de la santé et de la police, et n'a jamais cessé d'intervenir dans le processus législatif en émettant près de 100 avis sur des projets de loi affectant la protection des données.

La DPA a également promu des réunions avec les parties intéressées concernant la mise en œuvre de nouvelles règles de la directive « vie privée et communications électroniques » et l'utilisation de GPS dans le contexte de l'emploi.

En ce qui concerne les activités de sensibilisation, il convient de souligner que les efforts déployés par la DPA depuis 2007, en développant un projet dédié et structuré s'adressant aux enfants dans les écoles (le projet DADUS), ont donné lieu à une augmentation des aides du gouvernement. En 2012, le ministère de l'Éducation a formellement introduit les questions de la protection des données et de la vie privée dans les objectifs des programmes d'informatique. Cette discipline est enseignée à tous les élèves de 5e et de 4e (12 à 14 ans). C'est la raison pour laquelle le projet DADUS fait l'objet d'examens visant à mieux tenir compte de cette nouvelle réalité, en vertu de laquelle la DPA jouera un rôle de soutien plutôt que directeur.

Organisation	Commission nationale de protection des données
Président et/ou collège	Corps collégial composé de 7 membres : Filipa Calvão (président), Luís Barroso, Ana Roque, Carlos Campos Lobo, Helena Delgado António, Vasco Almeida, Luís Paiva de Andrade
Budget	Budget initial alloué : 2 324 352,00 EUR Budget d'État : 1 193 885 EUR Recettes propres à la DPA : 1 130 467 EUR (réellement reçus : 1 556 838 EUR) Budget exécuté : 1 445 188,45 EUR
Personnel	25
Activités générales	
Décisions, avis, recommandations	12 006 décisions contraignantes (dont 10 083 autorisations de

	traitement des données, délibérations sur des procédures d'infraction et délibérations sur des demandes d'accès aux données par des tierces parties, droit d'accès prévu par la convention de Schengen, etc.)
Notifications	11 306
Examens préalables	10 325
Demandes émanant des personnes concernées	Chiffres non disponibles (les services de première ligne traitent les demandes émanant des personnes concernées et des responsables du traitement des données)
Plaintes émanant des personnes concernées	588 (procédures formelles ouvertes)
Conseils sollicités par le Parlement ou le gouvernement	90 avis préalables sur des projets de loi contenant des dispositions sur la protection des données
Autres renseignements relatifs aux activités générales	13 504 nouvelles procédures (notifications, plaintes, avis, infractions, accès par des tierces parties, etc.) ; 130 demandes concernant l'exercice du droit d'accès et de suppression du Système d'information Schengen (accès indirect par le biais de la DPA) ; 684 demandes d'avis de la part d'opérateurs de télécommunications concernant la levée de la confidentialité de l'appelant dans les cas d'appels dérangeants.
Activités d'inspection	
Contrôles, enquêtes	1 005 enquêtes démarrées (procédures d'infraction), dont 359 contrôles exécutés sur place
Activités de sanction	
Sanctions	169 amendes appliquées par la DPA
Amendes	± 283 000 EUR
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Aucune jurisprudence pertinente pour ce rapport.

C. Autres informations importantes :

www.cnpd.pt

RÉPUBLIQUE TCHÈQUE

A. Résumé des activités et actualités

Nous avons reçu une **bourse** de la part du programme de partenariat Leonardo da Vinci pour un projet international de sensibilisation aux questions de protection des données parmi les employés travaillant au sein de l'UE. Le but était 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 prendra fin en juillet 2014.

Du 12 au 14 mars 2012, nous avons accueilli en notre bureau **une visite d'étude de trois jours** pour trois membres de la DPA albanaise. Cet événement financé par le TAIEX portait sur la gestion des plaintes, les procédures d'investigation, l'enregistrement, les activités et les services de presse.

Les 11 et 12 juin 2012, l'un de nos experts a participé en tant qu'orateur au **séminaire du TAIEX** sur les inspections et le respect de la protection des données organisé par la DPA macédonienne à Skopje.

Lors de la Journée européenne de la protection des données, nous avons lancé la sixième édition du **concours destiné aux enfants et aux jeunes**, intitulé « C'est ma vie privée ! Interdiction de regarder et de fouiner ! » conçu pour sensibiliser les jeunes générations au respect de la vie privée. Cette fois, nous nous sommes concentrés sur l'utilisation d'Internet et avons encouragé les compétiteurs à réfléchir aux conséquences sur la vie privée en soumettant un essai, un récit, un clip vidéo ou une bande dessinée. Nous avons reçu 67 contributions, dont trois ont été récompensées.

Organisation	Bureau de la protection des données à caractère personnel – République tchèque
Président et/ou collège	Dr Igor Němec, Président
Budget	146 219 000 CZK = 5 665 207 EUR (taux de change d'août 2013 à 25,81 CZK/EUR)
Personnel	97 membres du personnel permanents (dont une dizaine participe à la gestion et la comptabilité et n'est donc pas directement concernée par la protection des données).
Activités générales	
Décisions, avis, recommandations	12 avis (principaux sujets : vidéosurveillance, Internet, marketing). Publication d'une méthodologie approfondie pour les responsables du traitement exploitant des systèmes de vidéosurveillance (également disponible en anglais).
Notifications	5 169 notifications (dont 4 618 enregistrées). Le nombre de responsables du traitement ayant formulé une notification s'élève à 3 397 (certains ont notifié plusieurs opérations de traitement).
Examens préalables	105

Demandes émanant des personnes concernées	2 503 (dont 47 de la part de personnes étrangères). Des consultations ont été demandées non seulement par des personnes physiques, mais également par des personnes morales et des autorités publiques.
Plaintes émanant des personnes concernées	Plaintes : 1 319 (dont 197 à des fins de plus amples investigations, 69 pour raison de procédure administrative, 13 transferts vers d'autres administrations publiques, et 1 040 déclinées comme étant injustifiées). 7 933 plaintes ont par ailleurs été reçues pour des courriels non sollicités (dont 3 772 accomplies).
Conseils sollicités par le Parlement ou le gouvernement	Le Parlement a demandé conseil en deux occasions : sur les dossiers passagers (PNR) et sur le projet de règlement sur la protection des données.
Autres renseignements relatifs aux activités générales	Dans le cadre de la **procédure de commentaires interministériels** à laquelle nous avons participé, nous avons évalué et commenté 85 lois et 94 projets de règlements d'application.
Activités d'inspection	
Contrôles, enquêtes	129 contrôles (enquêtes) initiés, 9 accomplis (mais commencés l'année précédente). Ce chiffre n'inclut pas les actions relatives aux courriels non sollicités (spams). Dans ce domaine, 87 contrôles ont été initiés et accomplis (plus un qui avait été initié l'année précédente).
Activités de sanction	
Sanctions	49 sanctions. En outre, nous avons également imposé 3 sanctions dans le domaine des spams. Note explicative : Par « sanctions », on entend toute mesure corrective non financière imposée au responsable du traitement. Dans le cadre de nos investigations, 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	125 amendes, dont 23 pour des courriels non sollicités.
DPD	
Chiffres relatifs aux DPD	Sans objet. Les DPD ne sont pas ancrés dans loi tchèque sur la protection des données.

B. Informations sur la jurisprudence

Nous avons lancé, sur la base d'une demande, un **contrôle au sein de la Poste tchèque**. Les livreurs avaient été équipés d'un système GPS visant à contrôler leurs allées et venues. La Poste tchèque a déclaré avoir introduit ce système afin de pouvoir gérer les plaintes de clients déclarant que les livreurs ne leur avaient pas livré leur colis / courrier recommandé. Nous avons établi que le traitement de données à caractère personnel (le contrôle des employés de terrain) n'avait aucun fondement juridique et que la Poste tchèque avait enfreint la loi sur la protection des données. La Poste tchèque a fait appel de cette décision en 2012. L'affaire a par conséquent été portée devant un tribunal administratif.

Nous avons réalisé un **contrôle au sein d'une chaîne de pharmacies** sur la base de la plainte d'un client concernant l'emploi de données à caractère personnel stockées sur la carte du client. L'inspecteur soupçonnait une violation de la loi sur la protection des données et, plus précisément, de deux articles relatifs à la liquidation des données et aux droits de la personne concernée. La société traitait également des données sensibles de ses clients. L'objectif officiel de ce traitement était la gestion des dossiers médicaux des clients afin de détecter les contre-indications, les interactions des médicaments prescrits ou les allergies. Toutes les données étaient collectées avec le consentement écrit de la personne concernée. L'enquête a révélé que la société avait mis en place des mesures organisationnelles et techniques suffisantes, mais qu'elle ne détruisait pas immédiatement les données sur demande du client ou après annulation de la carte du client. La raison en était la formation insuffisante du personnel. La défaillance a été éliminée immédiatement pendant l'enquête. Aucune sanction ou amende n'a par conséquent été imposée.

Un double contrôle a été mené à l'hôpital de Prague. La première partie du contrôle a été initiée en vertu du plan de contrôle annuel et a porté sur le marquage des patients à l'aide de bracelets d'identification. L'autre partie du contrôle a porté sur une plainte faisant suite à la mise en ligne de la vidéo d'une opération et des données à caractère personnel du patient (prénom, nom de famille partiel, date de naissance) permettant son identification. Concernant les bracelets, ils sont distribués à chaque patient à la réception. Ils sont bleus pour les patients « standard » et jaunes pour les patients dont le diagnostic est plus préoccupant. Ces bracelets contiennent différentes données sur l'identification, le diagnostic et le traitement, etc. Le code-barres de ces bracelets ne peut être lu qu'à 10-20 cm, ce qui interdit toute possibilité de suivre les allées et venues des patients au sein de l'hôpital. Pour ce qui touche à la mise en ligne de la vidéo, la direction de l'hôpital a présenté un formulaire contenant le consentement éclairé du patient en question. Elle a également déclaré que divulguer la date de naissance du patient n'était pas l'objet primaire du processus et a retiré l'intégralité des images d'Internet. L'inspecteur en a conclu qu'en aucun cas la loi sur la protection des données n'avait été enfreinte.

Une autre inspection a été menée auprès d'une **association de logement** qui publiait en ligne (en accès libre) une liste de ses membres-créditeurs contenant leurs noms et prénoms et le montant de leur dette. L'association est autorisée à conserver la preuve de dettes sans le consentement de ses créditeurs en vertu de la disposition correspondante de la loi sur la protection des données selon laquelle les données à caractère personnel peuvent être traitées en cas de nécessité pour la protection des droits et intérêts juridiques du responsable du traitement. D'un autre côté, ce type de traitement ne saurait être en désaccord avec le droit de la personne concernée à la protection de sa vie privée. Le traitement en question n'aurait pas été en contradiction avec ce droit de la personne concernée si l'accès aux données avait été limité aux membres de l'association que sont les créditeurs concernés. Le consentement des créditeurs aurait été nécessaire avant qu'une divulgation sans restriction soit possible en ligne. Par conséquent, en publiant la liste de créditeurs et le montant de leurs dettes sur son site Internet accessible à tout le monde, l'association de logement a enfreint la loi sur la protection des données. Le bureau a imposé une amende financière à l'association. Le responsable du traitement a pris une mesure corrective en protégeant l'accès à la page incriminée à l'aide d'un mot de passe.

D'autres cas intéressants sont décrits en détails dans le rapport annuel de la DPA tchèque, dont la version anglaise est disponible sur : http://www.uoou.cz/uoou.aspx?menu=159&lang=en.

C. Autres informations importantes

Nous avons commencé l'année 2012 dotés d'une nouvelle compétence concernant les **notifications de violations de données** dans le domaine des communications en ligne. À ces fins, nous avons créé une rubrique spéciale sur le site Internet du bureau présentant la liste des règlements applicables, une explication des obligations et des formulaires de notification (un pour les notifications de violation du bureau, un autre pour les notifications des personnes concernées). Au total, nous n'avons reçu qu'une notification dans la période de référence (en 2013, nous n'avons également reçu qu'une notification à l'heure de cette publication).

Les inspecteurs ont mené des contrôles auprès de trois **ambassades et consulats** de la République tchèque (en Russie, en Turquie et au Kazakhstan). Ceux-ci ont porté sur le traitement de données à caractère personnel au cours des formalités de visa et dans le système d'information Schengen. La sécurité physique des bases de données a également été contrôlée.

Nous avons reçu 18 demandes de **transfert international de données**, aucune n'a été refusée, 13 ont été approuvées et cinq ont été suspendues pour des raisons de procédure.

ROUMANIE

A. Résumé des activités et actualités

Organisation	Autorité nationale de contrôle du traitement des données à caractère personnel
Président et/ou collège	Georgeta Basarabescu
Budget	3 320 000 RON (environ 751 131 EUR)
Personnel	42, plus la Présidente et le Vice-président de l'autorité
Activités générales	
Décisions, avis, recommandations	834, dont 2 décisions normatives
Notifications	10 014
Examens préalables	-
Demandes émanant des personnes concernées	59
Plaintes émanant des personnes concernées	667
Conseils sollicités par le Parlement ou le gouvernement	51
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	131 sur place et 41 par écrit
Activités de sanction	
Sanctions	24 amendes pour un montant total de 36 000 RON (environ 8 115 EUR)
Amendes	84 avertissements
DPD	
Chiffres relatifs aux DPD	-

B. Informations sur la jurisprudence

Jurisprudence 1

S'appuyant sur plusieurs notifications d'un requérant, l'autorité de protection des données a réalisé une série d'enquêtes auprès du responsable du traitement des données d'un prestataire de services Internet et téléphoniques.

Ces enquêtes avaient pour objet de vérifier la manière dont le traitement des données relatives au trafic des abonnés/internautes était exécuté par le responsable du traitement et, notamment, concernant l'activation, les désabonnements et le fonctionnement du service MyClicknet.

Suite à plusieurs enquêtes, il s'est avéré que le responsable du traitement des données utilisait le service MyClicknet pour personnaliser la navigation sur Internet de ses abonnés/utilisateurs afin de fournir des publicités comportementales, et d'analyser et de traiter les données relatives au trafic en installant des cookies sur les ordinateurs de ses abonnés/utilisateurs avant qu'ils n'aient accepté ce service.

Les opérations susmentionnées devaient être réalisées en conformité avec les dispositions des articles 4 et 5 de la loi n° 506/2004.

L'autorité de la protection des données a demandé des preuves du consentement préalable éclairé obtenu par écrit au sens des dispositions de la loi n° 506/2004.

Le responsable du traitement des données n'a pas pu présenter ces preuves et les conditions générales de la prestation de services par le responsable du traitement des données ne contenaient pas de clause susceptible d'être assimilée à un consentement explicite et éclairé à ce traitement.

Le responsable du traitement des données n'a pas non plus été à même de présenter la preuve de l'obtention du consentement éclairé des abonnés/utilisateurs quant à l'option de retrait des cookies installés, avant et après la présentation de la page d'invitation.

Suite à ces enquêtes, une amende a été imposée pour ce qui suit :

1. le non respect de l'article 4, alinéa 2, de la loi n° 506/2004, dans la mesure où le responsable du traitement des données a intercepté les communications et les données relatives au trafic de ses abonnés/utilisateurs sans respecter une seule des conditions stipulées à l'article 4, alinéa 2, points a) à c) de la loi n° 506/2004 ;
2. le non respect des conditions prévues à l'article 4, alinéa 5, et à l'article 5 de la loi n° 506/2004 concernant le traitement des données relatives au trafic de ses abonnés/utilisateurs dans le but d'offrir la valeur ajoutée du service MyClicknet, qui implique l'utilisation du réseau de communication électronique pour stocker les informations sur son terminal et obtenir l'accès à ces informations (en installant des cookies), sans obtenir au préalable le consentement explicite et éclairé et avant de présenter la page d'invitation permettant l'expression du consentement ou du désaccord vis-à-vis de l'activation des services MyClicknet, et après, pour l'installation du cookie de refus pour les personnes ayant refusé de donner leur consentement.

Jurisprudence 2

De nombreux requérants se sont plaints de pages Internet de plusieurs tribunaux (disponibles via portal.just.ro) contenant plus de données à caractère personnel que nécessaire. Suite aux enquêtes de l'autorité de la protection des données, le non respect des dispositions de la loi n° 677/2001 a été avéré et des recommandations ont été adressées au ministère de la Justice et au Conseil supérieur de la magistrature concernant la manière dont les tribunaux utilisaient l'application ECRIS, requérant :

a) la détermination précise des données à caractère personnel strictement nécessaires à l'accomplissement de l'objet des sites des tribunaux, conformément aux principes de protection des données, selon lesquels les données doivent être adéquates, pertinentes et non excessives (divulgation des seuls nom et prénom des parties au jugement) ;

b) l'élaboration, au niveau central, d'instructions uniformes sur le traitement des données à caractère personnel, applicables à tous les utilisateurs de l'application ECRIS sous l'autorité du responsable du traitement des données ;

c) la formation des employés travaillant sous l'autorité des responsables du traitement des données concernant les dispositions de la loi n° 677/2001, surtout en ce qui concerne le traitement de données à caractère personnel au sein de l'application ECRIS, le portail des tribunaux ;

d) l'examen de l'ensemble des enregistrements effectués jusqu'ici dans l'application ECRIS, conformément aux recommandations susmentionnées, ainsi que la suppression des données à caractère personnel qui ne respectent pas les conditions de légitimité du traitement de données à caractère personnel ;

e) une période de conservation des données à caractère personnel que contient l'application ECRIS, le portail des tribunaux, qui soit limitée et proportionnée, conformément au Code de procédure civile, au Code de procédure pénale et à la loi sur les archives nationales ;

f) la protection adéquate des données à caractère personnel contre la destruction accidentelle ou illégale, la perte, l'altération, la divulgation ou l'accès non autorisé.

Les plaintes reçues ont été favorablement résolues, les données à caractère personnel excessives publiées par les tribunaux ayant été effacées.

Jurisprudence 3

Les contrôles de plusieurs responsables du traitement de données réalisés suite à ces plaintes ont révélé que les heures de travail des employés pouvaient être enregistrées par des méthodes moins intrusives que l'utilisation de données biométriques. Avant l'introduction du système biométrique, les heures de travail étaient enregistrées grâce à la signature d'un registre de présence et à l'utilisation de cartes d'accès. Même après l'introduction du système biométrique, certains employés devaient encore signer le registre de présence.

Les responsables du traitement des données concernés ont été sanctionnés par une amende pour les contraventions commises en vertu des articles 31 et 32 de la loi n° 677/2001. Par ailleurs, le président de l'autorité de protection des données a décidé que les responsables devaient mettre un terme au traitement des données biométriques des employés et supprimer les données biométriques déjà collectées.

L'enquête de suivi réalisée suite à une plainte selon laquelle les responsables du traitement des données ne respectaient pas les mesures prévues par l'autorité de protection des données n'a pas confirmé le fondement de la plainte.

C. Autres informations importantes

Plusieurs propositions législatives transmises à l'autorité de protection des données ont reçu un avis négatif en raison de leur non conformité avec les principes constitutionnels et la réglementation, avec

les actes juridiques de l'Union européenne, avec les traités dont la Roumanie est partie ou avec la législation cadre.

L'ensemble de ces aspects ont empêché l'émission d'un avis favorable, l'autorité de protection des données proposant la reconsidération et la reformulation des projets d'actes normatifs.

Exemples de règlements pour lesquels l'autorité de protection des données a émis des avis négatifs :

- un projet de loi sur la conservation des données générées ou traitées par les fournisseurs de réseaux de communications électroniques accessibles au public ou de réseaux de communications publics ;
- une proposition législative concernant la collecte et le stockage des données d'identification des clients de services de communications électroniques fournis par le biais de cartes prépayées.

Traitement des données à caractère personnel des utilisateurs de cartes prépayées

L'autorité de la protection des données a émis un avis négatif concernant une proposition législative sur la collecte et le stockage des données nécessaires à l'identification de clients de services de communications électroniques fournis via des cartes prépayées. Cette proposition législative était en contradiction avec les principes établis par la Convention 108 du Conseil de l'Europe, ainsi qu'avec les dispositions de la directive 95/46/CE, de la directive 2006/24/CE et de la directive 2009/136/CE concernant le service universel et les droits des utilisateurs de réseaux et services de communications électroniques.

Par ailleurs, la proposition législative enfreignait le droit des personnes à la vie privée (établi en vertu de l'article 26 de la Constitution roumaine, dans sa forme republiée). Le traitement du numéro d'identification personnel (CNP) pouvait se faire conformément aux conditions prévues à l'article 8 de la loi n° 677/2001 et aux dispositions de la décision 132/2011 ; toutefois, la manière dont la proposition législative a été élaborée constituait une violation sérieuse des principes de proportionnalité et de conservation des données énoncés par la directive 95/46/CE et la loi n° 677/2001.

L'autorité de la protection des données a considéré qu'en établissant l'obligation de communiquer également les données d'identification des personnes ayant déjà acquis un service de communications électroniques avant l'entrée en vigueur de la loi proposée, la proposition enfreignait le principe de non rétroactivité des lois établi en vertu de l'article 15, alinéa 2, de la Constitution roumaine.

La proposition législative enfreignait également le droit des consommateurs à prendre des décisions informées dans le cadre de l'acquisition de services de communications prépayés, dans la mesure où imposer l'obligation d'identification aurait pu influencer le choix du client par rapport à l'acquisition ou non du service.

ROYAUME-UNI

A. Résumé des activités et actualités :

Organisation	Bureau du Commissaire à l'information du Royaume-Uni
Président et/ou collège	Commissaire à l'information : Christopher Graham
Budget	20 millions de GBP par an
Personnel	330 ETP
Activités générales	
Décisions, avis, recommandations	Éducation et orientation L'ICO (bureau du commissaire à l'information) a publié un code de bonnes pratiques sur la gestion des risques inhérents à la protection des données et à l'anonymisation ; elle est la première autorité de la protection des données européenne à publier un code sur cette question. L'ICO a également publié de nouvelles directives sur l'informatique en nuage, la suppression des données à caractère personnel et la destruction d'actifs. Nous avons aussi consulté le public sur un nouveau code de bonnes pratiques en matière d'accès des personnes concernées. Activités des médias L'ICO a reçu 1 673 appels de journalistes et répondu à 113 interviews dans les médias. Nous avons également publié 50 communiqués de presse qui ont généré une vaste couverture de presse, généralement positive. 900 mises à jour et ajouts ont été apportés au site web de l'ICO et 45 documents de conseils ont été publiés ou substantiellement mis à jour.
Notifications	372 369
Examens préalables	s. o.
Demandes émanant des personnes concernées	213 813 réponses à des appels sur la ligne d'assistance de l'ICO 29 042 réponses à des demandes de conseils écrites
Plaintes émanant des personnes concernées	20 515 (toutes concernant la loi sur la protection des données de 1998 et la réglementation sur la vie privée et les communications électroniques 2003/11)

Conseils sollicités par le Parlement ou le gouvernement	L'ICO fait preuve d'un engagement constant aux côtés du gouvernement pour dispenser des conseils sur la législation en matière de protection des données en apportant des preuves au Parlement et en répondant aux consultations. Résumé des activités déployées cette année : Preuves parlementaires Commission judiciaire restreinte – Avis sur les propositions cadres de l'Union européenne en matière de protection des données ; Comité des affaires écossaises – Enquête sur l'établissement de listes noires sur le marché de l'emploi. Réponses aux consultations Cabinet du Conseil — Introduction d'un registre légal de lobbyistes Conseils aux citoyens — Consultation sur l'avenir des consommateurs Intérêt des consommateurs — Propositions d'une unité des industries réglementées Département des communautés et du gouvernement local — Fraude aux logements sociaux Département de l'éducation — Propositions d'amendements des règlements sur les personnes interdites d'accès aux informations sur les élèves Département de l'environnement et du changement climatique — Accès aux données intelligentes et vie privée Département de la santé — Consultation sur le renforcement de la constitution de la NHS (service national de santé) Département de la justice (NI) — Faire la différence : Améliorer l'accès à la justice pour les victimes et les témoins d'un crime : une stratégie quinquennale Procureur général — Lignes directrices intérimaires pour les procureurs sur l'évaluation de l'intérêt public dans les affaires affectant les médias Services des douanes britanniques — Mise en œuvre de l'accord FATCA entre le Royaume-Uni et les États-Unis Ministère de l'intérieur — Loi sur la protection des libertés de 2012 — Consultation sur le code de bonnes pratiques en matière de vidéosurveillance Commission des lois — Consultation pour outrage au tribunal Barreau — Réforme de la loi sur les taxis et les VTC Ministère de la justice — Un système plus juste pour les victimes et

	les témoins Ministère de la justice — Transformer la réhabilitation — une révolution dans la manière dont nous traitons les délinquants Ministère de la justice — Une justice rapide et sûre : les plans du Gouvernement pour la réforme du système juridique pénal Nominet — Consultation sur un nouveau service de noms de domaine .uk Bureau national des statistiques — Stratégie de future diffusion des publications de statistiques nationales sur le crime en Angleterre et au Pays de Galles L'enquête Leveson — Réponse au rapport sur la culture, les pratiques et l'éthique de la presse Gouvernement gallois — Enregistrement et supervision de l'enseignement à domicile Gouvernement gallois — Projet de loi sur la transplantation humaine (Pays de Galles) et exposé des motifs Gouvernement gallois — Assistance à la taxe d'habitation au Pays de Galles
Autres renseignements relatifs aux activités générales	Conférence annuelle des délégués à la protection des données de l'ICO Le Commissaire à l'information a accueilli à Manchester plusieurs centaines de délégués à la protection des données du Royaume-Uni pour la cinquième conférence annuelle des délégués à la protection des données. David Smith, Commissaire adjoint et Directeur de la protection des données, a prononcé un discours liminaire informant les participants des derniers développements européens en vue de l'actualisation du droit actuellement applicable. Développements européens L'ICO a publié son analyse initiale sur la réforme de la protection des données européenne en février 2012. L'ICO a organisé une réunion des parties intéressées au printemps 2012 et travaillé avec d'autres acteurs politiques concernés et le ministère de la Justice afin de sensibiliser aux nouvelles propositions de l'UE et d'en examiner les implications. Application Sur l'année écoulée, le montant des amendes imposées par l'ICO en vertu de la loi sur la protection des données et de la réglementation sur la vie privée et les communications électroniques dépasse les 2,6 millions de GBP (avant toute réduction pour paiement anticipé). À une exception, les amendes imposées en vertu de la loi sur la

	protection des données l'ont été pour ne pas avoir assuré la sécurité d'informations personnelles. Dans le domaine de la mise en application, le travail le plus médiatisé de l'ICO a été celui de nos actions visant à résoudre le problème des appels impromptus et des spams par SMS. Au mois de mars, nous avons mis en place un outil de compte rendu en ligne permettant aux personnes concernées de nous signaler des messages qu'elles reçoivent. Plus de 155 000 personnes ont utilisé cet outil afin de nous communiquer des informations que nous utilisons ensuite dans le cadre de nos enquêtes. Audit et bonnes pratiques L'ICO a introduit des rapports de résultats qui synthétisent les thèmes d'audits communs, et a souligné les bonnes pratiques et les domaines à améliorer dans les secteurs privé, de la santé, du gouvernement local, du gouvernement central, de la police et de la probation. Nous avons diffusé les bonnes pratiques en donnant des présentations sur les audits et leurs résultats lors de forums. Nous avons également développé et organisé un atelier de visite consultative centrale qui nous a permis de toucher un nombre accru d'organisations. L'ICO a demandé à plus de 400 écoles de compléter un questionnaire sur la protection des données. Nous nous sommes ensuite servis des résultats pour produire un rapport indiquant les bonnes pratiques et les domaines à améliorer, et donnant des conseils pratiques sur l'application de la loi sur la protection des données. Assurer une sensibilisation efficace dans toutes les régions En février, la série d'ateliers pratiques organisés à travers tout le Pays de Galles par l'ICO et mettant en lumière les bonnes pratiques de base en matière de gestion des données à caractère personnel a rencontré un grand succès. Nous avons ciblé le personnel du secteur public et du troisième secteur en première ligne de la prestation de services comme étant peut-être moins expérimenté dans le domaine de la protection des données, en nous appuyant sur des exemples de bonnes et de mauvaises pratiques dévoilés par l'audit de l'ICO et les services chargés de l'application. Protection des données dans le secteur de la santé L'ICO a participé au groupe de révision de la gouvernance de l'information du Département de la santé. L'ICO espère que ce travail contribuera à transformer la gouvernance de l'information dans un domaine qui touche aux détails personnels les plus

	sensibles. Anonymisation L'ICO a organisé et financé le réseau d'anonymisation britannique, lancé parallèlement au nouveau code de pratiques sur l'anonymisation de l'ICO. Ce réseau a pour objet de permettre le partage des bonnes pratiques d'anonymisation et l'identification des solutions aux obstacles, au moyen d'un site web, d'événements et de réseaux sociaux, ainsi que d'études de cas. Suite à un processus d'appel d'offres, le financement de l'exploitation du réseau a été adjugé au consortium de l'Université de Manchester, de l'Université de Southampton, du Bureau national des statistiques et de l'Institut des données ouvertes. Enquête Leveson — Presse et vie privée Les intrusions dans la vie privée par la presse représentent actuellement un point important de l'ordre du jour du Gouvernement et des régulateurs indépendants britanniques. Le bureau du commissaire à l'information a fait une déclaration préliminaire précédant sa réponse officielle au rapport Leveson faisant suite à l'enquête Leveson (dirigée par le juge de la Haute Cour Lord Justice Leveson) sur la culture, les pratiques et l'éthique de la presse au Royaume-Uni. Nous avons participé à l'enquête et rendu compte de nos précédents travaux dévoilant le rôle des médias dans le commerce illégal des informations personnelles. Notre futur travail aura pour toile de fond les plans du gouvernement en matière de réglementation des médias à l'avenir.
Activités d'inspection	
Contrôles, enquêtes	58 audits et 35 suivis d'audit. 78 visites consultatives
Activités de sanction	
Sanctions	23
Amendes	17 engagements, 2 avis d'exécution, 6 poursuites
DPD	
Chiffres relatifs aux DPD	La loi sur la protection des données de 1998 exige que chaque responsable du traitement (organisation, représentant exclusif) traitant des informations personnelles s'inscrive auprès de l'ICO, sauf en cas d'exemption. Plus de 370 000 organisations sont actuellement inscrites.

B. Informations sur la jurisprudence

—

C. Autres informations importantes

La loi britannique sur la protection des libertés de 2012 contient les dispositions suivantes en lien avec les activités de l'ICO :

Partie 1 ; réglementation des données biométriques. Cette partie comprend des dispositions relatives à la destruction, la conservation et l'utilisation des empreintes digitales, empreintes de chaussures, échantillons et profils d'ADN. Elle contient également des dispositions sur la protection des informations biométriques des écoliers.

Partie 2 ; réglementation de la vidéosurveillance et autres technologies de caméras de surveillance. Cette réglementation donnera lieu à la désignation d'un nouveau Commissaire aux caméras de surveillance.

Partie 3 ; prévient la protection de propriété de toute mesure d'application disproportionnée. Ces réglementations ont trait aux pouvoirs d'entrée, aux pouvoirs d'application des règles de stationnement et à la potentielle augmentation de l'emploi de la technologie RAPM (reconnaissance automatique des plaques minéralogiques).

Partie 5 ; sauvegarde des groupes vulnérables et des casiers judiciaires. Cette partie introduit également le service de divulgation et de blocage (qui remplace et combine les responsabilités du Bureau des casiers judiciaires et de l'autorité de sauvegarde indépendante). Cette partie prévoit également de passer outre certains délits sexuels.

Partie 6 ; modifications de la loi sur la protection des données de 1998. Ces modifications portent sur :

- La désignation et la prorogation du mandat du Commissaire à l'information de cinq à sept ans ;
- L'altération du rôle du Secrétaire d'État dans le cadre des pouvoirs d'orientation ;
- La suppression du consentement du Secrétaire d'État pour les pouvoirs de tarification ;
- La suppression de l'approbation du Secrétaire d'État pour les effectifs et les conditions d'emploi.

SLOVAQUIE

A. Résumé des activités et actualités

2012 peut être décrite comme une année de changements et de propositions législatives fructueuses. 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.

Cet amendement législatif 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, ainsi que l'analyse juridique du point de vue de l'application pratique.

À partir de janvier 2012, le Bureau a introduit des services hebdomadaires de contrôle et d'évaluation de documents inclus au processus législatif dans le cadre de la procédure d'examen interministérielle. Ce processus a pour objet de suivre de manière continue tous les documents inclus à la procédure d'examen interministérielle 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 le respect des exigences de base de la vie sociale protégées par la loi tout en minimisant les interférences avec le droit à la vie privée et la vie privée des personnes. À ces fins, chaque projet de législation qui 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.

Activités d'inspection du Bureau à l'échelle nationale

En 2012, le Bureau a réalisé plusieurs opérations d'inspection à l'échelle nationale sur la base du plan annuel des activités de contrôle. Lors de la planification du plan annuel des activités de contrôle, le Bureau s'est focalisé sur le contrôle des données à caractère personnel traitées par les responsables du contrôle et du traitement dans le contexte de systèmes d'archivage reflétant le développement des relations sociales et de la législation sur la protection des données à caractère personnel.

Copie de documents officiels dans les demandes de prime fiscale

En 2012, le Bureau a enquêté sur la licéité du traitement de données à caractère personnel afin d'établir le droit à une prime fiscale en vertu de la loi sur les revenus dans quatre bureaux du fisc sélectionnés en République slovaque. Lors de son enquête, le Bureau s'est aperçu que les autorités fiscales obtenaient des données à caractère personnel afin d'établir une prime fiscale, et copiaient et stockaient les documents officiels de particuliers. À l'heure de cette enquête, la loi sur les impôts sur le revenu ne permettait toutefois pas de copier ni de stocker les documents officiels à ces fins. Cette attitude des autorités fiscales constituait par conséquent une violation de l'article 10, alinéa 6, de la loi n° 428/2002 Coll. sur la protection des données à caractère personnel.

Traitement de données à caractère personnel par des agences immobilières

En 2012, quatre agences immobilières ont fait l'objet d'inspections par le Bureau. Ces inspections avaient pour objet d'examiner les activités de ces agences immobilières en tant que responsables du traitement de données à caractère personnel aux fins de conclure des contrats de location ou des contrats d'achat de propriétés et les saisies correspondantes sur le cadastre et l'enregistrement de propriété. Lors des ces inspections, le Bureau s'est aperçu que les responsables du traitement obtenaient certaines données à caractère personnel des personnes concernées en copiant des documents officiels. Cette collecte de

données à caractère personnel n'était pas nécessaire aux fins du traitement en vertu de l'article 6, alinéa 1, point d, en relation avec l'article 10, alinéa 6, de la loi n° 428/2002 Coll.

Traitement de données à caractère personnel par des orphelinats

En 2012, le Bureau a enquêté sur le niveau de protection des données à caractère personnel traitées en vertu de la loi n° 305/2005 Coll. sur la protection socio-légale et le placement social des enfants, et sur la modification et l'amendement d'autres lois, telles qu'amendées, dans cinq orphelinats sélectionnés en tant que responsables du traitement de données. Ces inspections ont révélé des erreurs au niveau des systèmes d'archivage et de la communication d'informations aux personnes habilitées.

Traitement de données à caractère personnel par des structures d'hébergement

En 2012, le Bureau a également contrôlé le traitement de données à caractère personnel par des structures d'hébergement en vertu de la loi n° 253/1998 Coll. sur la notification de résidence des citoyens de la République slovaque et le registre de la population en République slovaque, telle que modifiée, et la loi n° 404/2001 Coll. sur la résidence des ressortissants étrangers, telle que modifiée. Des activités de contrôle ont été réalisées par le Bureau auprès de cinq responsables du traitement de données sélectionnés.

Traitement de données à caractère personnel par des agences de voyage

En 2012, le Bureau s'est également intéressé au traitement de données à caractère personnel par des agences de voyage en tant que responsables du traitement de données de systèmes d'archivage. Ces activités d'inspection avaient pour objet l'examen du statut de la protection des données à caractère personnel et de la conformité des termes de leur traitement, en particulier, aux fins de la conclusion de contrats de voyage. Le respect des procédures administratives a été vérifié par le Bureau dans le cas de cinq responsables du traitement. Les activités de contrôle ont démontré que, pendant la période contractuelle, deux bases juridiques étaient applicables au traitement de données à caractère personnel : le consentement de la personne concernée et la nécessité des données à caractère personnel pour l'exécution d'un contrat auquel la personne concernée est partie en vertu de l'article 7, alinéa 4, point b, de la loi n° 428/2002 Coll.

Flux transfrontalier de données à caractère personnel

En 2012, le Bureau a formulé vingt-cinq approbations de transferts de données à caractère personnel vers des pays tiers n'offrant pas un niveau de protection des données adéquat. Ces approbations étaient principalement sollicitées par des multinationales établies en République slovaque, et les données personnelles en question étaient pour la plupart liées aux employés, clients et partenaires commerciaux des responsables du traitement de données.

Coopération internationale

Au niveau international, les activités étaient principalement liées à l'adhésion à l'Union européenne et aux groupes de travail établis sous l'égide et à partir des actes juridiques de l'Union européenne.

Au printemps 2012, le Bureau a organisé une réunion de travail à la demande du Bureau serbe du Plénipotentiaire pour la protection des données à caractère personnel et des informations d'importance publique. Cette réunion a été organisée en collaboration avec le Centre afin de partager les expériences d'intégration et de réforme de l'Agence slovaque de coopération internationale au développement au sein du ministère des Affaires étrangères et européennes de la République slovaque.

La réunion avait pour objet la consultation d'experts sur des sujets définis dans les domaines du traitement de données à caractère personnel en République slovaque à des fins de marketing direct, du traitement de données à caractère personnel sur des supports électroniques, de publication de données à caractère personnel par des responsables du traitement de données dans les domaines judiciaire, des

institutions publiques locales, des médias, du traitement de catégories spéciales de données à caractère personnel et de l'agenda international prévu par le Bureau. Ces consultations ont été suppléées par des exemples de pratiques du Bureau.

Organisation	
Président et/ou collège	JUDr. Eleonóra Kročianová
Budget	876 324 EUR
Personnel	34 employés
Activités générales	
Décisions, avis, recommandations	
Notifications	200
Examens préalables	0
Demandes émanant des personnes concernées	Pendant la période évaluée, le Bureau a enquêté sur 5 demandes émanant de personnes concernées qui exerçaient leur droit à l'information découlant de l'article 20 de la loi n° 428/2002 Coll. concernant le statut du traitement de leurs données à caractère personnel et concernant la source à partir de laquelle le sous-traitant avait obtenu leurs données à caractère personnel. Le sous-traitant est obligé de respecter les exigences des personnes concernées et de les informer par écrit du statut du traitement de leurs données à caractère personnel. En tout état de cause, les investigations du Bureau ont prouvé que la notification des personnes concernées était légitime et que les responsables du traitement avaient par conséquent enfreint leur obligation légale.
Plaintes émanant des personnes concernées	Pendant la période évaluée, le Bureau a reçu 200 notifications émanant de personnes physiques demandant la protection de leurs droits et de leurs intérêts protégés par le droit. Le Bureau a également reçu 52 notifications d'autres personnes relativement à des suspicions concernant des violations de la loi sur la protection des données personnelles. Pendant la période évaluée, le Bureau a enquêté sur 321 notifications et suggestions et a mené 69 procédures de sa propre initiative. Ces procédures concernaient des sujets du secteur privé comme du secteur public. Afin de remédier aux déficiences identifiées, le Bureau a pris 131 mesures au total. Sur un total de 252 notifications et suggestions relatives à la violation de la loi n° 428/2002 Coll. ayant fait l'objet d'investigations, 4 auteurs de notifications ont exercé leur droit à porter plainte dans le délai légal de 30 jours. Dans 3 cas, le Bureau en a reporté le traitement conformément à la loi en raison de

	l'absence de nouveaux faits.
Conseils sollicités par le Parlement ou le gouvernement	
Autres renseignements relatifs aux activités générales	La priorité en 2012 a été le changement de direction du Bureau et, par conséquent, la consolidation subséquente de l'établissement des employés. Une autre priorité du Bureau a été la mise en œuvre des acquis de Schengen. Enfin, le travail législatif sur la nouvelle loi de protection des données à caractère personnel a représenté une part importante des activités du Bureau.
Activités d'inspection	
Contrôles, enquêtes	Pendant la période évaluée, le Bureau a effectué 112 contrôles au total. Les activités de contrôle du Bureau ont été déployées sur la base du plan annuel d'activités de contrôle du Bureau. Avec la planification des activités de contrôle, le Bureau souhaitait connaître le statut effectif du traitement des données à caractère personnel par les responsables du traitement des données, leurs sous-traitants et personnes habilitées et la conformité du traitement des données à caractère personnel avec les règlements juridiques d'application générale et documents internationaux auxquels la République slovaque est partie. Les domaines traités par le Bureau reflétaient la situation effective et pratique en matière de protection des données à caractère personnel et les problèmes potentiels avec l'application de la loi n° 428/2002 Coll. et d'une autre loi spécifique. Le Bureau a observé l'augmentation du nombre de problèmes survenant lors du traitement de données à caractère personnel pendant la période évaluée. Ces problèmes étaient liés à l'utilisation de caméras vidéo, essentiellement par des personnes physiques. Dans le cadre des activités de contrôle, le Bureau a également participé à la coordination de la coopération avec les DPA étrangères affiliées. Dans le cadre de la supervision, sur demande de la DPA affiliée de la République de Hongrie, le Bureau a vérifié le statut de la protection des données à caractère personnel au sein de sociétés fournissant des services de centre d'appel.
Activités de sanction	
Sanctions	
Amendes	Dans le cadre des activités de contrôle, le Bureau a essentiellement souhaité faire de la prévention, ce qui a donné lieu à des sanctions minimes des responsables du traitement de données et de leurs sous-traitants. Pendant la période évaluée, le Bureau a imposé 5 amendes pour un montant total de 8 050 EUR.
DPD	

Chiffres relatifs aux DPD	42 411

B. Informations sur la jurisprudence

2012 a mis un terme à un long procès entre le Bureau et une société qui collectait des données à caractère personnel, les traitait et déployait des activités liées à la collecte extrajudiciaire de plaintes et autres activités associées pour un sous-traitant qui, en tant qu'établissement non bancaire, fournissait des prêts financiers non liés. Ce sous-traitant avait formulé une requête en révision et, par la suite, une requête d'annulation d'une décision administrative du Bureau imposant une amende au sous-traitant pour la divulgation non autorisée de données à caractère personnel alors que le sous-traitant notait sur des enveloppes postales des informations sur le fait que le destinataire était un fraudeur fiscal et dévoilait ainsi de manière illicite des données à caractère personnel des personnes concernées sur leur identité économique. Le tribunal a jugé que la décision du Bureau était correcte sur les plans factuel et légal, et conforme au droit applicable.

C. Autres informations importantes

La protection des données à caractère personnel fait partie intégrante du droit à la vie privée des personnes et est l'un des droits et libertés fondamentaux garantis par la Constitution de la République slovaque. Le droit à la protection des données à caractère personnel est un domaine récent qui affiche toutefois une évolution rapide. Vingt ans se sont écoulés depuis l'établissement de la République slovaque. Au cours de ces années, la protection des données à caractère personnel a néanmoins vu son rôle et son importance croître dans la pratique, en raison, principalement, du développement des plateformes sociales et de l'expansion des technologies de l'information. Ces influences ont eu un impact important sur la connaissance de la législation dans le domaine de la protection des données à caractère personnel. De nouveaux défis et demandes ont influencé les mesures liées au traitement, au transfert et à l'accès à des quantités de données à caractère personnel de plus en plus importantes.

La supervision des données à caractère personnel traitées sur le territoire de la République slovaque a été confiée au Bureau dès le 1er septembre 2002 par la loi n° 428/2002 Coll. qui, dans le cadre des ses compétences, contrôle le statut de la protection des données à caractère personnel. L'évaluation du statut de la protection des données à caractère personnel peut être considérée comme un processus à long terme et continu, déployé dans le cadre de l'exécution de chaque tâche du Bureau et, notamment, des consultations publiques ou d'experts et des activités d'inspection du Bureau. Pendant la période en question, le principal problème était l'exécution adéquate des tâches et la pénurie concomitante de ressources, tant humaines que financières.

Sur la base d'expériences passées, le Bureau a conclu que la question de la protection des données à caractère personnel n'était pas un sujet bien maîtrisé. Le résultat des activités d'investigation du Bureau et le grand nombre de questions du public quant à l'application de la loi indiquent l'absence de connaissance et d'application des règles de protection des données à caractère personnel dans la pratique, surtout pour les petites et moyennes entreprises et les autorités publiques locales, qui ont également été confrontées à une évolution défavorable de la situation économique et à des initiatives d'économie des ressources.

D'un autre côté, grâce aux récentes évolutions sociales et technologiques, les statistiques liées aux performances du Bureau montrent une conscience accrue de l'existence du droit à la protection des données à caractère personnel et un intérêt à assurer un traitement des données qui soit à la fois légal et sûr. Ces circonstances particulières ont évolué indépendamment des activités du Bureau, entraînant une augmentation et une amélioration des principes de précaution et de prévention de la part des personnes physiques. La sensibilisation du public peut dès lors être considérée comme une première étape dans l'exécution des obligations relevant du domaine de la protection des données à caractère personnel et dans l'exercice des droits des personnes concernées dans la vie de tous les jours.

Généralement parlant, la situation de la protection des données à caractère personnel en République slovaque a été satisfaisante pour la période en question. Il est néanmoins dans l'intérêt de l'ensemble des personnes concernées que la protection des données à caractère personnel des personnes physiques atteigne, avec de nouveaux développements, le niveau et la qualité requis.

SLOVÉNIE

A. Résumé des activités et actualités

Nous pourrions qualifier l'année 2012 d'ambitieuse pour ce qui concerne les plans de l'État en matière d'informatisation accrue des grandes bases de données publiques suite à une procédure expéditive, et l'appétit croissant du secteur public pour un traitement de données à caractère personnel toujours plus important. Il est alarmant de constater que l'État, qui aurait dû protéger la vie privée conformément à la Constitution slovène, essaie d'éroder les fondations de la loi sur la protection des données.

Le Commissaire à l'information a dû traiter plus de 80 propositions d'amendements de la législation sur la collecte et le traitement des données à caractère personnel, soit une augmentation de plus d'un tiers par rapport à 2011. Nombre de ces propositions constituent selon nous une tentative de légalisation d'un niveau disproportionné de collecte et de traitement de données à caractère personnel, qui ne contribuera pas à la simplification des procédures administratives ou des mesures d'austérité, mais aura au contraire pour effet de réduire le niveau de protection de la vie privée des citoyens. Parmi les lois en voie d'amendement, figurent la loi sur les communications électroniques, la loi sur l'action de la police et les autorités, la loi sur la réglementation du marché du travail, la loi sur les héritages, la loi sur les marchés publics et la loi sur l'administration publique. La plupart des propositions d'amendements montrent une absence complète d'évaluation de l'impact sur la protection des données qui aurait dû être présentée dans le contexte des nouvelles activités de traitement des données prévues. Il semble que la crise financière n'ait pas touché le secteur de l'informatisation autant que les autres domaines du secteur public. Au contraire, de nombreuses informatisations prévues sont synonymes de coûts considérables.

Le Commissaire à l'information a traité un nombre extrêmement élevé de cas dans les deux domaines d'activité concernant des demandes d'avis, des plaintes ou des recours. Ces circonstances ont un côté positif, dans la mesure où elles prouvent que les personnes sont mieux informées et sensibilisées vis-à-vis de l'objet et de l'importance de ces deux droits de l'homme dont la mise en œuvre et la protection font partie des compétences du Commissaire à l'information. D'un autre côté, cette augmentation du nombre de recours et d'affaires liés aux inspections peut également être imputée à certaines actions inquiétantes de la part des autorités responsables dans le domaine de l'accès aux informations publiques, d'une part, et de l'important (voire même trop important) appétit des divers responsables du traitement de données des secteurs privé et public en matière de traitement de données à caractère personnel.

Nonobstant l'augmentation du nombre d'affaires, le Commissaire à l'information fait son possible pour obtenir un niveau accru de réactivité et de professionnalisme ; toutefois, compte tenu du nombre croissant d'affaires traitées, cet objectif reste difficile à atteindre. Nous sommes néanmoins heureux d'annoncer que nous y sommes de nouveau parvenus en 2012, le public ayant reconnu nos efforts en faveur de la protection de ces deux droits fondamentaux, à savoir le droit à l'accès aux informations publiques et le droit à la protection des données à caractère personnel, et ayant de nouveau, sur l'année écoulée, exprimé sa confiance envers le Commissaire à l'information.

D'après les recherches du Centre de recherche sur l'opinion publique et la communication de masse, le niveau de confiance accordée au Commissaire à l'information en janvier 2013 était une nouvelle fois relativement élevé (52 %), soit le niveau de confiance le plus élevé parmi les quatre organismes de surveillance examinés. Les précédentes mesures ayant déjà démontré un niveau de confiance élevé et ce pourcentage ayant toujours été supérieur à 50 %, c'est un niveau de confiance continu qui est ainsi clairement exprimé, ce qui explique notre grande satisfaction et nous pousse à poursuivre notre travail tout en cherchant des manières de nous améliorer.

Concernant le domaine de la protection des données à caractère personnel pour l'année 2012, le Commissaire à l'information a traité 725 enquêtes (+ 6 % par rapport à 2011) et 158 procédures de délits (+ 16 % par rapport à 2011). En termes d'évolution, nous souhaiterions souligner le fait que l'informatique en nuage occupe une position de plus en plus importante en termes de protection des données et de développement technologique. L'informatique en nuage présente un vaste potentiel, ce qui ne devrait toutefois pas faire peser de menace sur le niveau de protection des données à caractère personnel, qui reste un droit humain fondamental. En 2012, le Commissaire a publié, avec le chapitre slovène de la Cloud Security Alliance (CSA), le chapitre slovène de l'ISACA et Eurocloud Slovénie, des lignes directrices pour la protection des données dans l'informatique en nuage, en sa qualité de l'une des premières autorités de l'UE à contribuer à l'établissement de normes appropriées dans ce domaine ([15]). Ce document a pour objet d'établir des points de contrôle communs en vertu desquels les utilisateurs et les autorités de supervision pourront prendre des décisions éclairées quant à l'utilisation et la surveillance des services de l'informatique en nuage, notamment lorsque le traitement de données à caractère personnel est concerné. Les initiatives en faveur d'une utilisation plus sûre et de certifications pour les services en nuage, d'un autre côté, bénéficient pour leur futur développement de lignes directrices ayant pour objet d'assurer la conformité avec la législation sur la protection des données à caractère personnel. Le Commissaire à l'information estime que de nombreux prestataires de services en nuage n'offrent pas encore à leurs clients prospectifs toutes les informations nécessaires pour faire un choix éclairé. Des mécanismes doivent encore être mis en place afin de permettre la différenciation entre les prestataires de confiance et les autres.

Organisation	Commissaire à l'information de la République de Slovénie
Président et/ou collège	Mme Nataša Pirc Musar
Budget	1 610 000 EUR
Personnel	33 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 (10), chercheurs et conseillers sur la protection des données (4), contrôleurs de la protection des données (10).
Activités générales	Protection des données et accès aux informations publiques
Décisions, avis, recommandations	143 avis exhaustifs et 2 048 avis et recommandations concis sur la base de demandes émanant des personnes concernées ou de responsables du traitement des données.
Notifications	153 notifications relatives à des fichiers de données à caractère personnel.
Examens préalables	23 examens préalables : 7 sur des données biométriques, 5 sur le transfert de données vers des pays tiers et 12 sur le regroupement de fichiers.
Demandes émanant des	2 048 demandes d'avis ou d'éclaircissements de la part de

([15]) https://www.ip-rs.si/index.php?id=308

personnes concernées	personnes concernées.
Plaintes émanant des personnes concernées	747 plaintes émanant de personnes concernées au total, 497 plaintes qualifiées. Domaines : 226 plaintes pour le transfert ou la divulgation illicite de données, 144 pour la collecte illicite de données, 118 pour des activités de marketing direct, 72 pour des activités de vidéosurveillance, 44 sur la sécurité des données, 153 liées à d'autres sujets. En outre, 63 plaintes sur les droits des personnes concernées ont également été traitées.
Conseils sollicités par le Parlement ou le gouvernement	Le législateur et les autorités compétentes chargées de rédiger les projets législatifs ont consulté le Commissaire au sujet de 80 lois et autres textes législatifs, parmi lesquels la loi sur les communications électroniques, la loi sur l'action de la police et les autorités policières, la loi sur la réglementation du marché du travail, la loi sur les héritages, la loi sur les marchés publics, la loi sur l'administration publique, etc.
Autres renseignements relatifs aux activités générales	En 2011, le Commissaire : - a poursuivi son travail de prévention (exposés, conférences) en collaboration avec le Centre slovène pour un Internet plus sûr ; - a participé à des groupes de travail interservices sur des projets d'administration en ligne, tels que sur les identités électroniques ; - a publié des lignes directrices sur les outils de protection des données en ligne et un rapport spécial sur les cartes de fidélité ; - a été consulté sur un certain nombre de lois ; - a poursuivi son implication et sa participation active à nombre de projets internationaux.
Activités d'inspection	
Contrôles, enquêtes	725 contrôles : 245 dans le secteur public, 480 dans le secteur privé.
Activités de sanction	
Sanctions	158 procédures de délits initiées (29 dans le secteur public, 78 dans le secteur privé, 51 personnes physiques), ayant notamment donné lieu à 17 avertissements, 61 réprimandes, 58 amendes et 7 injonctions de paiement.
Amendes	La DPA a imposé des amendes à hauteur de 50 037 EUR, hors taxes administratives.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Données sur les impressions réalisées par les employés

Le Commissaire à l'information a reçu une plainte selon laquelle la direction d'un organisme public avait demandé une liste de tous les employés et de leur utilisation des imprimantes de leur lieu de travail (noms, prénoms, nombre d'impressions, titres des documents). Lors de la procédure de contrôle, il a été établi que l'organisme devait maîtriser ses coûts d'impression et utilisait pour ce faire une application visant à établir que les employés utilisaient les imprimantes de manière irrationnelle, non écologique, et à des fins personnelles. Le Commissaire a conclu que l'organisme n'aurait pas dû collecter les données sur les titres des documents ou le nom des sites Internet imprimés, qui sont des données à caractère personnel non nécessaires pour gérer de manière efficace les processus et les coûts des impressions dont l'organisme a besoin. Le Commissaire a ordonné que ces données ne soient plus collectées et que l'application soit adaptée, tandis que l'organisme a, pour sa part, décidé de ne plus faire appel à cette application.

Collecte de données à des fins de marketing direct en ligne

Le Commissaire à l'information a reçu un certain nombre de plaintes concernant un responsable du traitement faisant du marketing direct par courriel, prétendument sans le consentement des personnes au traitement de leurs données à caractère personnel. Lors de la procédure de contrôle, il a été établi que le responsable du traitement conservait dans ses bases de données les données de plus de 100 000 personnes, utilisateurs inscrits sur son site web et utilisateurs de certaines applications Facebook. Le Commissaire a conclu que le responsable du traitement avait présenté suffisamment de preuves qu'il avait obtenu le consentement des utilisateurs inscrits sur son site mais n'avait en revanche pas présenté suffisamment de preuves concernant les utilisateurs des applications Facebook qui étaient censés avoir donné leur consentement en installant différentes applications. Lorsqu'un utilisateur installe une application Facebook, les serveurs du responsable du traitement devraient par défaut avoir enregistré certaines données de base telles que l'heure d'installation, l'adresse IP ou autres données similaires. Le responsable du traitement n'ayant présenté aucune preuve mais ayant simplement déclaré que la seule existence de ces données dans ses bases de données attestait du fait que les utilisateurs avaient donné leur consentement, le Commissaire a ordonné la suppression des données. Le responsable du traitement s'est exécuté.

Mesures biométriques dans un centre de remise en forme

Le Commissaire à l'information a reçu une plainte à l'encontre d'un centre de remise en forme réalisant des contrôles biométriques de ses clients souhaitant entrer dans ses locaux et ayant installé des caméras de vidéosurveillance dans ses vestiaires. Lors de la procédure d'inspection, il a été établi que le centre de remise en forme contrôlait effectivement les données biométriques des clients entrant dans ses locaux, mais que les clients avaient le choix entre une carte à puce sans données biométriques et le contrôle biométrique, qui comprenait un modèle d'empreinte digitale des clients. Le responsable du traitement ne stockait pas les empreintes digitales des clients, mais seulement les modèles, et ne pensait pas que cette activité relevait du régime du traitement des données biométriques. Le Commissaire a expliqué que ce stockage de modèles constitue une activité de traitement de données biométriques. Il a ordonné au centre de remise en forme de mettre un terme au traitement de données biométriques parce qu'aucun fondement juridique ne justifiait ce traitement. La PDPA-1 autorise uniquement, dans certaines conditions, la mise en œuvre de mesures biométriques d'employés et non de clients. Il a également été établi que le centre de remise en forme surveillait les vestiaires au moyen de caméras, ce qui est interdit par la loi. Le Commissaire a ordonné au centre de mettre un terme à la vidéosurveillance des vestiaires ou de s'assurer que les clients disposent d'autres pièces pour changer de vêtements sans être surveillés.

Les visiteurs d'un site de jeux de hasard en ligne redirigés sur une autre adresse Internet

Le Commissaire a initié une procédure à l'encontre du Bureau de surveillance des jeux de hasard qui avait enregistré un domaine sur lequel étaient redirigés tous les visiteurs de sites de jeux de hasard exploités sans concession du gouvernement. Lors de la procédure d'inspection, il a été établi que le responsable du traitement ne disposait d'aucune base juridique pour collecter et traiter les informations des visiteurs de sites de jeux de hasard exploités sans concession du gouvernement. La loi sur les jeux de hasard ([16]) prévoit que l'accès à ces sites Web peut être limité, mais ne prévoit aucun traitement de données des visiteurs de telle manière qu'ils soient redirigés sur le site du responsable du traitement et que leurs données (telles que leur adresse IP, l'heure de leur visite, les détails de leur navigateur, etc.) soient traitées par le responsable du traitement de cette manière. Le Commissaire à l'information a jugé que les adresses IP, au même titre que les détails afférents au navigateur, sont des données à caractère personnel qui fournissent une empreinte numérique unique des visiteurs. Le Commissaire a ordonné au responsable du traitement de supprimer de ses bases de données les données pouvant identifier chaque visiteur et de ne plus collecter ces données à l'avenir. Le responsable du traitement s'est exécuté et a déposé un recours auprès du tribunal administratif contre la décision du Commissaire. Le tribunal ne s'est pas encore prononcé sur le fond de l'affaire.

Traitement de données à caractère personnel par un service de location de bicyclettes, BicikeLJ

Le Commissaire à l'information a reçu plusieurs plaintes concernant un nouveau service de location de bicyclettes, BicikeLJ, dont le responsable du traitement des données avait demandé des détails personnels aux utilisateurs souhaitant s'inscrire au service, dont certains n'étaient pas nécessaires à la prestation du service. Lors de la procédure d'inspection, il a été établi que le responsable du traitement collectait et traitait différentes données à caractère personnel sur la base du type de service demandé par l'utilisateur et du type de paiement (carte de crédit ou débit direct). La base légale est le contrat conclu entre l'utilisateur et le prestataire de service. Il a été établi que dans aucun des cas le responsable du traitement n'a pu démontrer qu'il avait besoin, pour honorer sa part du contrat, de données sur le sexe et le numéro de téléphone portable des utilisateurs. Par ailleurs, le responsable du traitement ne devrait pas demander l'adresse du domicile des utilisateurs payant par carte de crédit. Le Commissaire a établi que ces données pouvaient être collectées et traitées sur la base du consentement de l'utilisateur, mais que ce consentement devait être donné librement et que l'utilisateur devait avoir le choix de fournir ces données au prestataire de service ou non, dans la mesure où elles ne sont pas nécessaire à l'exécution du contrat de location de bicyclettes. Le responsable du traitement s'est exécuté et a déposé auprès du tribunal administratif un recours contre la décision du Commissaire.

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 2012, le Commissaire à l'information a participé activement à six 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 :

([16]) Journal Officiel Gazette RS, n° 27/1995 47/2006, s spremembami, v nadaljevanju ZEN.8427/15527 et les amendements correspondants.

- 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, déplacement 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 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 (EURODAC).

En 2012, le Commissaire à l'information a conservé ses fonctions de Vice-président de l'autorité de contrôle commune d'Europol. En février 2012, un Commissaire à l'information adjoint a participé au groupe d'inspection international qui a contrôlé la protection des données à caractère personnel au siège d'Eurojust à La Haye. Le Commissaire à l'information a également participé régulièrement au Groupe de travail international sur la protection des données dans les télécommunications (IWGDPT). Une fois encore en 2012, un représentant du Commissaire à l'information a participé au comité consultatif du Conseil de l'Europe (T-PD) à la Convention pour la protection des personnes sur le sujet du traitement automatique des données à caractère personnel (Convention 108).

En 2012, le Commissaire à l'information a accueilli des représentants d'institutions similaires de plusieurs pays tels que la Serbie, la Géorgie, la Macédoine et l'Albanie, auxquels il a présenté ses activités et bonnes pratiques dans ses domaines de compétence. En tant que Partenaire junior, il a mené à son terme le projet de jumelage IPA 2009, n° MN/09/IB/JH/03 (sur la mise en œuvre de la stratégie de protection des données à caractère personnel au Monténégro) et a lancé la mise en œuvre du projet de jumelage allégé SR/2009/IB/JH/01 (pour l'amélioration de la protection des données à caractère personnel en Serbie).

En 2012, le Commissaire à l'information a poursuivi et terminé, en septembre, son travail au sein du projet européen LAPSI (sur les aspects juridiques des informations du secteur public), qui a vocation 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.

SUÈDE

A. Résumé des activités et actualités :

Supervision

En 2012, la supervision a porté sur le traitement de données à caractère personnel en relation avec l'administration en ligne, les données de santé et médicales, la recherche, l'aide sociale, l'application de la loi, les informations confidentielles sur les écoliers, les bases de données sur les compétences, les données des partis politiques sur leurs membres et les applications de smartphones dans le secteur bancaire, etc.

Sensibilisation

Les articles consacrés à notre activité dans les médias ont encore battu des records en 2012. Les questions émanant du public ont également beaucoup augmenté en nombre, que ce soit par téléphone, par courriel ou par le biais de visites sur notre site web. Comme les années précédentes, nous avons publié une brochure portant sur les questions de respect de la vie privée les plus importantes, intitulée Respect de la vie privée en 2012.

Organisation	Conseil de l'inspection des données
Président et/ou collège	Directeur Général M. Göran Gräslund (depuis le 1er juin 2013, la Directrice Générale est Mme Kristina Svahn Starrsjö)
Budget	36 931 000 SEK = 3 987 841 EUR
Personnel	Environ 45
Activités générales	
Décisions, avis, recommandations	115 avis sur des propositions législatives, à la demande des bureaux de l'administration 68 avis en consultation avec des fonctionnaires chargés de la protection des données 6 lignes directrices, recommandations et rapports
Notifications	
Examens préalables	247 (la plupart concernant la recherche et le traitement des données d'ADN)
Demandes émanant des personnes concernées	Notre service d'assistance : 8 000 appels téléphoniques, 5 600 courriels Demandes formelles : 219
Plaintes émanant des personnes	323

concernées	
Conseils sollicités par le Parlement ou le gouvernement	Voir les décisions, avis, etc. ci-dessus
Autres renseignements relatifs aux activités générales	Communiqués de presse : 69, Exposés et séminaires : 52
Activités d'inspection	
Contrôles, enquêtes	267 (contrôles finalisés) (43 contrôles sur place, 143 du bureau et 81 par questionnaire) Principaux sujets abordés : la police, la vidéosurveillance, les publications sur Internet, les applications bancaires, les bases de données sur les compétences, les données secrètes des écoles, des partis politiques et de leurs membres
Activités de sanction	
Sanctions	---
Amendes	Sans objet
DPD	
Chiffres relatifs aux DPD	6 825

B. Informations sur la jurisprudence

Dans une décision de mars 2012, la Cour administrative suprême a rejeté un appel de deux écoles secondaires supérieures qui avaient installé des caméras de surveillance à l'intérieur de leurs locaux. Le Conseil de l'inspection des données a ordonné aux écoles de mettre un terme à leur vidéosurveillance dans la journée. Le Conseil a déclaré que la vidéosurveillance ne pouvait être autorisée qu'en cas de besoin substantiel d'une telle surveillance prévalant sur le droit des étudiants à ne pas être surveillés. Les écoles ont fait appel de cette décision devant la Cour administrative suprême qui a rejeté cet appel. La Cour administrative suprême a confirmé cette décision et déclaré que l'emploi de caméras de surveillance dans les salles de classe, les couloirs, la bibliothèque, les salles de récréation de l'école, etc. devait être généralement considéré comme une violation de la vie privée des personnes concernées. Le Conseil de l'inspection des données a depuis lors produit une liste de contrôle visant à permettre aux écoles d'évaluer plus facilement si l'emploi de caméras de surveillance est autorisé ou non d'après la loi sur les données à caractère personnel.

Dans une autre affaire, la Cour administrative suprême a confirmé la décision du Conseil de l'inspection des données ordonnant au bureau d'assurance sociale de procéder à une évaluation des risques et de la vulnérabilité de leur service de messagerie textuelle rendant compte des congés maladies pour l'obtention de prestations sociales. Cette décision de la Cour administrative suprême a confirmé le point de vue du Conseil de l'inspection des données selon lequel il incombait au bureau d'assurance sociale de décider de l'objet et des moyens du traitement et que celui-ci était dès lors responsable du traitement des données à caractère personnel impliqué par le service de messagerie textuelle.

Chapitre Trois

Union européenne et Activités communautaires

3.1. COMMISSION EUROPÉENNE

3.1.1. **Proposition de la Commission en faveur d'un règlement du Parlement européen et du Conseil** COM(2012) 11 du 25 janvier 2012 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données **(règlement général sur la protection des données).**

3.1.2. **Proposition de la Commission en faveur d'une directive du Parlement européen et du Conseil** COM(2012) 10 du 25 janvier 2012 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

3.1.3. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions COM(2012) 09 : Protection de la vie privée dans un monde en réseau – Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle.

3.1.4. **Document de travail des services de la Commission** SEC(2012) 75 du 25 janvier 2012 : Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, fondé sur l'article 29, paragraphe 2, de la décision-cadre 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. La Commission européenne a proposé une réforme exhaustive des règles de l'UE de 1995 en matière de protection des données afin de renforcer le droit à la vie privée en ligne et de favoriser l'économie numérique européenne. Les progrès technologiques et la mondialisation ont profondément changé la manière dont nos données sont collectées, accessibles et utilisées. En outre, les 27 États membres de l'UE ont mis en œuvre les règles de 1995 différemment, ce qui a entraîné des divergences d'application. Une seule loi permettra d'en finir avec l'actuelle fragmentation et les coûteux fardeaux administratifs, et se traduira par des économies d'environ 2,3 milliards d'EUR par an pour les entreprises. Cette initiative permettra en outre de renforcer la confiance des consommateurs dans les services en ligne, ce qui favorisera la croissance, qui en a bien besoin, ainsi que l'emploi et l'innovation en Europe. Les propositions de la Commission visent à mettre à jour et à moderniser les principes de la directive de 1995 relative à la protection des données afin de garantir le droit à la vie privée à l'avenir. La communication politique définit les objectifs de la Commission et deux propositions législatives : un **règlement** établissant un cadre général de l'UE pour la protection des données et une **directive** relative à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière et autres activités judiciaires.

La réforme a pour principaux objectifs, notamment, la création d'un **ensemble unique de règles** sur la protection des données, valides dans l'ensemble de l'UE. Les **exigences administratives** non nécessaires, telles que les exigences de notification pour les sociétés, seront supprimées. L'économie pour les entreprises devrait s'élever à près de 2,3 milliards d'EUR par an. En lieu et place de l'actuelle obligation de toutes les sociétés de notifier toute activité de protection des données aux contrôleurs de la protection des données (une exigence qui implique de remplir des documents non nécessaires et entraîne des coûts pour les entreprises estimés à hauteur de 130 millions d'EUR par an), le règlement prévoit d'accroître **la responsabilité et l'obligation de rendre compte** des personnes traitant des données à caractère personnel.

Sociétés et organisations devront dès lors aviser l'autorité de contrôle nationale de sérieuses **violations de données** au plus vite (dans les 24 heures si possible). Les organisations n'auront plus à traiter qu'avec une **seule autorité nationale de protection des données** dans le pays européen où se trouve leur établissement principal. De la même manière, les personnes peuvent s'adresser à **l'autorité de protection des données** de leur pays, même lorsque leurs données sont traitées par une société sise en dehors de l'UE.

Dès lors que leur **consentement** est requis pour que les données puissent être traitées, il est clair qu'il doit être obtenu de manière explicite, plutôt que présumé. Toute personne devrait bénéficier plus facilement

d'un **accès à ses propres données** et pouvoir **transférer ses données à caractère personnel** d'un prestataire de services à un autre plus facilement (droit à la portabilité des données). Cette mesure devrait favoriser la concurrence entre les services. Le **« droit à l'oubli »** aidera les personnes à mieux gérer les risques inhérents à la protection des données en ligne en leur permettant de supprimer leurs données s'il n'existe aucun motif légitime de les conserver. Les règles de l'UE s'appliqueront si les données à caractère personnel sont **traitées à l'étranger** par des sociétés actives sur le marché de l'UE et qui offrent leurs services aux citoyens européens.

Les autorités nationales de protection des données indépendantes seront renforcées afin de pouvoir mieux appliquer les règles européennes à domicile. Aux sociétés coupables de violations des règles de protection des données européennes, elles pourront imposer des amendes à hauteur de 1 million d'EUR maximum, ou de 2 % du chiffre d'affaires annuel global de la société.

La nouvelle **directive** appliquera les règles et principes généraux de protection des données pour la **coopération policière et judiciaire** en matière pénale. Ces règles s'appliqueront aux transferts de données aussi bien domestiques que transfrontaliers.

3.1.5. **Conférence** du 19 mars 2012 sur la vie privée et la protection des données à caractère personnel, Washington, DC / Bruxelles.

Cette conférence, organisée simultanément à Washington et à Bruxelles, a offert aux parties concernées américaines et européennes des secteurs public et privé l'opportunité d'obtenir des informations exhaustives, précises et à jour sur les principes de la protection des données en Europe et sur la réforme en cours, et de discuter des perspectives américaines et européennes en matière de vie privée des entreprises.

3.1.6. **Accord** du 1er juin 2012 entre **l'Union européenne et l'Australie** sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières — L 186, 14/07/2012, p. 4.

Cet accord prévoit que les données peuvent être envoyées au service australien des douanes et de la protection des frontières uniquement à des fins de prévention et de détection d'infractions terroristes et de formes graves de criminalité transnationale, ainsi que d'enquêtes et de poursuites en la matière. Il contient des définitions de ces infractions pour une meilleure compréhension de son champ d'application. Les données PNR que les autorités australiennes peuvent utiliser sont énumérées en annexe de l'accord.

Le service australien des douanes et de la protection des frontières ne peut avoir accès aux données des dossiers passagers européens que sur la base de transferts de ces données par les transporteurs aériens via la méthode « push ».

La protection des données à caractère personnel et le droit des personnes à demander l'accès et la rectification de leurs données à caractère personnel s'appliquent indépendamment de leur nationalité ou de leur lieu de résidence.

L'examen périodique de la mise en œuvre de l'accord, y compris son efficacité opérationnelle, aura lieu quatre ans après son entrée en vigueur.

Les données sensibles (telles que les données à caractère personnel susceptibles d'indiquer l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, l'appartenance syndicale ou encore l'état de santé ou la vie sexuelle) seront filtrées et supprimées par le service australien des douanes et de la protection des frontières ; il convient toutefois de noter que, normalement, les dossiers passagers ne contiennent pas de données sensibles.

L'accord prévoit une période de conservation des données de cinq ans et demi, sachant que les données sont masquées au bout de trois ans.

Le service australien des douanes et de la protection des frontières cherchera à garantir le partage des informations analytiques tirées des données PNR européennes avec les autorités compétentes des États membres de l'UE et, dans les cas appropriés, avec Europol et Eurojust, afin de favoriser la coopération policière et judiciaire entre l'Australie et l'UE et d'améliorer la réciprocité.

L'accord a une durée de sept ans afin de garantir une longue période de sécurité juridique, et pourra être renouvelé pour une période supplémentaire de sept ans.

Il inclut des normes afin de contrôler la mise en œuvre correcte, l'examen et le règlement efficace des différends, et de veiller à ce que les modalités de transfert des données PNR visent à offrir une sécurité juridique aux transporteurs aériens et à garder les coûts à un niveau acceptable. Les données PNR devront être transférées en recourant à la méthode « push » et le nombre de transferts de ces données avant chaque vol est limité à cinq au maximum.

3.1.7. **Accord** du 1er juillet 2012 entre **l'Union européenne et les États-Unis d'Amérique** sur le traitement et le transfert des **données des dossiers passagers** (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure, Bureau des douanes et de la protection des frontières — L 215, 11 août 2012, p. 5.

D'après cet accord, les données PNR peuvent être envoyées au ministère américain de la sécurité intérieure (DHS) à des fins de prévention et de détection d'infractions terroristes et d'infractions pénales qui y sont liées, et d'autres infractions passibles d'une peine d'emprisonnement d'au moins trois années et de nature transnationale, ainsi que d'enquêtes et de poursuites en la matière. L'accord contient des définitions de ces infractions pour une meilleure compréhension de son champ d'application. Les données PNR que peuvent utiliser les autorités américaines sont énumérées en annexe de l'accord.

Les transporteurs aériens transfèrent les données PNR au DHS en utilisant la méthode « push ».

Tous les passagers, indépendamment de leur nationalité et de leur pays de résidence, ont accès aux mécanismes de recours dans le cadre des décisions administratives du DHS. La mise en application de l'accord fait l'objet d'examens périodiques. L'accord sera par ailleurs évalué conjointement quatre ans après son entrée en vigueur.

Les données sensibles (telles que les données à caractère personnel susceptibles d'indiquer l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou l'appartenance syndicale, ou les données relatives à l'état de santé ou à la vie sexuelle) seront filtrées et masquées, et ne sauraient être ultérieurement traitées ni utilisées, sauf dans des circonstances exceptionnelles lorsque la vie d'une personne pourrait être menacée ou mise gravement en péril. Il convient toutefois de noter que, normalement, les données PNR ne contiennent pas de données sensibles.

Les données peuvent être conservées cinq ans dans une base de données active et jusqu'à 10 ans dans une base de données dormante. Pendant cette période, les données sont progressivement dépersonnalisées et masquées, et leur accès est encore plus restreint.

Le ministère de la sécurité intérieure souhaite garantir le partage d'informations analytiques tirées des dossiers passagers européens avec les autorités compétentes des États membres de l'UE et, dans les cas appropriés, avec Europol et Eurojust, afin de favoriser la coopération policière et judiciaire entre les États-Unis et l'UE, et d'améliorer la réciprocité.

L'accord a une durée de sept ans afin de garantir une longue période de sécurité juridique, et pourra être renouvelé pour une période supplémentaire de sept ans.

3.1.8. **Décision d'exécution de la Commission** du 21 août 2012 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la République orientale de l'Uruguay concernant le traitement automatisé des données à caractère personnel (notifiée sous le numéro C(2012) 5704). Texte présentant de l'intérêt pour l'EEE— JO L 227, 23 septembre 2012.

Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, la République orientale de l'Uruguay est considérée comme assurant un niveau de protection adéquat des données à caractère personnel transférées à partir de l'Union européenne.

3.1.9. Document de travail des services de la Commission DTS (2012) 454 du 14 décembre 2012. Rapport sur le deuxième examen conjoint de la mise en œuvre de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme d'octobre 2012

Le deuxième examen a été réalisé conjointement par une équipe américaine et une équipe européenne. D'après l'article 13, paragraphe 3, la Commission représente l'UE dans le cadre des examens conjoints. L'équipe de l'UE en charge de cet examen était par conséquent dirigée par un haut fonctionnaire de la Commission et composée de trois membres du personnel de la Commission et de trois experts externes, à savoir deux experts de la protection des données et un expert judiciaire, qui ont aidé la Commission à examiner cet accord.

L'examen a été exécuté suivant deux grandes étapes : le 4 octobre 2012 à La Haye, au sein des locaux d'Europol, et les 30 et 31 octobre 2012 à Washington, au Département du Trésor des États-Unis (ci-après « le Trésor »).

Les deux équipes en charge de l'examen se sont tout d'abord rencontrées à La Haye, au siège d'Europol, et ont été informées, par les responsables et les experts de celle-ci, de la mise en œuvre et de l'application pratique de l'accord par Europol. Les équipes ont visité les lieux sécurisés où Europol traite les demandes des États-Unis et ont rencontré les personnes qui ont accès aux données en question.

Pour préparer la visite à Washington, l'équipe européenne a envoyé un questionnaire préalable au Trésor, avec des questions spécifiques sur l'ensemble des aspects de l'examen, tels que spécifiés dans l'accord. Le Trésor a fourni ses réponses au questionnaire par écrit. L'équipe de l'UE en charge de cet examen a également soumis d'autres questions aux représentants du Trésor afin de faire le tour de l'ensemble des paramètres de l'accord.

Les équipes en charge de l'examen ont eu accès aux locaux concernés du Trésor, y compris au site depuis lequel le TFTP est exécuté. Pour des raisons de sécurité, les membres de l'équipe en charge de l'examen ont dû présenter des preuves de leurs habilitations de sécurité avant d'avoir accès à ce site. Les équipes en charge de l'examen ont eu droit à une démonstration en direct des recherches réalisées sur les données fournies, les résultats étant affichés et expliqués à l'écran par les analystes, tout en respectant les exigences de confidentialité applicables aux États-Unis.

Les équipes en charge de l'examen ont eu des échanges directs avec le personnel du Trésor responsable du programme TFTP, les superviseurs qui examinent les recherches sur les données fournies en vertu de l'accord TFTP, et l'auditeur du TFTP à temps plein employé par le fournisseur désigné. Les équipes n'ont procédé à aucun examen ou contrôle du système sur la base des fichiers journaux.

L'équipe de l'UE en charge de l'examen est satisfaite du fait que les recommandations présentées dans le rapport de mars 2011 sur le premier examen conjoint ont été respectées dans une large mesure, ce qui a amélioré la mise en application de l'accord. Le défi qui consiste à fournir des informations plus vérifiables sur la valeur ajoutée réelle du TFTP, de préférence publiques, sans remettre en cause l'efficacité de cet instrument et en respectant la confidentialité nécessaire des méthodes et procédures appliquées, demeure entier.

L'équipe de l'UE en charge de l'examen a noté de nouvelles améliorations des mécanismes de vérification et de contrôle en particulier, dont certains dépassent les exigences de l'accord. Globalement, la mise en œuvre de l'accord plus de deux ans après son entrée en vigueur a atteint un niveau satisfaisant, l'UE en profitant par ailleurs de plus en plus grâce aux arrangements de réciprocité spécifiques.

3.1.10. **Décision d'exécution de la Commission** du 19 décembre 2012 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la Nouvelle-Zélande (notifiée sous le numéro C(2012) 9557). Texte présentant de l'intérêt pour l'EEE — JO L 28/12, 30 janvier 2013.

Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, la Nouvelle-Zélande est considérée comme assurant un niveau de protection adéquat des données à caractère personnel transférées à partir de l'Union européenne.

3.2. COUR DE JUSTICE DE L'UNION EUROPÉENNE

3.2.1. Arrêt de la Cour (troisième chambre) du 22 novembre 2012 — Josef Probst / mr.nexnet GmbH (Affaire C-119/12) : Par sa question, la juridiction de renvoi demandait si, et dans quelles conditions, l'article 6, paragraphes 2 et 5, de la directive 2002/58 permettait à un fournisseur de services de transmettre des données relatives au trafic au cessionnaire de ses créances, et à ce dernier de traiter lesdites données.

D'après l'article 6, paragraphe 2, de la directive 2002/58, les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées puisque cette disposition autorise le traitement des données relatives au trafic non seulement aux fins de l'établissement des factures, mais également aux fins de leur recouvrement. En autorisant le traitement des données relatives au trafic « jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement », cette disposition se rapporte non pas uniquement au traitement de données au moment de l'établissement des factures, mais également au traitement nécessaire aux fins d'obtenir leur paiement.

En vertu de l'article 6, paragraphe 5, de la directive 2002/58, le traitement des données relatives au trafic autorisé par l'article 6, paragraphe 2, « doit être restreint aux personnes agissant sous l'autorité des fournisseurs de [services] des réseaux publics de communications et des services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation » et « doit se limiter à ce qui est nécessaire » à une telle activité.

Il ressort qu'un fournisseur de services est autorisé à transmettre des données relatives au trafic au cessionnaire de ses créances en vue de leur recouvrement, et qu'il est permis au cessionnaire de traiter lesdites données à condition que, en premier lieu, il agisse « sous l'autorité » du fournisseur de services pour ce qui concerne le traitement desdites données et, en second lieu, il se limite à traiter les données relatives au trafic qui sont nécessaires aux fins du recouvrement desdites créances.

En l'absence d'éclaircissements quant à la portée exacte des termes « sous l'autorité », leur signification doit être déterminée en recourant au sens habituel de ceux-ci dans le langage courant, tout en tenant compte du contexte dans lequel ils sont utilisés et des objectifs poursuivis par la réglementation dont ils font partie. En langage courant, une personne agit sous l'autorité d'une autre personne lorsque la première agit sur instruction et sous contrôle de la seconde.

L'article 5, paragraphe 1, de la directive 2002/58 prévoit que les États membres doivent garantir la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public ainsi que des données relatives au trafic y afférentes. L'article 6, paragraphes 2 et 5, de la directive 2002/58 contient une exception à la confidentialité des communications prévue à l'article 5, paragraphe 1, en autorisant le traitement des données relatives au trafic au regard des impératifs liés aux activités de facturation des services. En tant qu'exception, cette disposition et les termes « sous l'autorité » sont d'interprétation stricte. Une telle interprétation implique que le fournisseur de services dispose d'un pouvoir de contrôle effectif lui permettant de vérifier le respect, par le cessionnaire des créances, des conditions qui lui sont imposées.

L'article 6, paragraphe 5, de la directive 2002/58 doit dès lors être interprété à la lumière des dispositions équivalentes de la directive 95/46, dont les articles 16 et 17 précisent le niveau de contrôle que le responsable du traitement doit exercer sur le sous-traitant qu'il désigne, que ce dernier agit sur la seule instruction du responsable du traitement et que ledit responsable veille au respect des mesures convenues pour protéger les données à caractère personnel contre toute forme de traitement illicite. Même si l'article 6, paragraphe 5, de la directive 2002/58 autorise le traitement des données relatives au trafic par certaines personnes tierces aux fins du recouvrement de créances, lui permettant ainsi de se concentrer sur la prestation des services de communications électroniques, cette disposition vise à garantir, en prévoyant que le traitement des données relatives au trafic doit être restreint aux personnes

agissant « sous l'autorité » du prestataire de services, qu'une telle externalisation n'affecte pas le niveau de protection des données à caractère personnel dont bénéficie l'utilisateur.

Par conséquent, le cessionnaire agit sur la seule instruction et sous le contrôle du fournisseur de services et le contrat conclu entre le fournisseur de services et le cessionnaire des créances doit garantir le traitement licite des données relatives au trafic par ce dernier et permettre au fournisseur de services de s'assurer, à tout moment, du respect desdites dispositions par le cessionnaire. Il incombe à la juridiction nationale de vérifier si ces conditions sont remplies.

La Cour a établi que l'article 6, paragraphes 2 et 5, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques ») doit être interprété en ce sens qu'il autorise un fournisseur de réseaux publics de communications et de services de communications électroniques accessibles au public à transmettre des données relatives au trafic au cessionnaire de ses créances portant sur la fourniture de services de télécommunications en vue du recouvrement de celles-ci, et ce cessionnaire à traiter lesdites données à condition que, en premier lieu, celui-ci agisse sous l'autorité du fournisseur de services pour ce qui concerne le traitement de ces mêmes données et, en second lieu, ledit cessionnaire se limite à traiter les données relatives au trafic qui sont nécessaires aux fins du recouvrement des créances cédées. Indépendamment de la qualification du contrat de cession, le cessionnaire est censé agir sous l'autorité du fournisseur de services, au sens de l'article 6, paragraphe 5, de la directive 2002/58, lorsque, pour le traitement des données relatives au trafic, il agit sur la seule instruction et sous le contrôle dudit fournisseur. En particulier, le contrat conclu entre eux doit comporter des dispositions de nature à garantir le traitement licite, par le cessionnaire, des données relatives au trafic et à permettre au fournisseur de services de s'assurer, à tout moment, du respect de ces dispositions par ledit cessionnaire.

3.2.2. Arrêt de la Cour (Grande Chambre) du 16 octobre 2012 — Commission Européenne / Autriche **(Affaire C-614/10) :** la Commission a initié une procédure à l'encontre de l'Autriche pour avoir transposé de façon erronée le second alinéa de l'article 28, paragraphe 1, de la directive 95/46 en ce que la réglementation nationale autrichienne ne permet pas à l'autorité de protection des données autrichienne, la Datenschutzkommission (DSK), d'exercer ses fonctions « en toute indépendance ». La Commission a déclaré que, le membre administrateur de la DSK devant nécessairement être un fonctionnaire de la chancellerie fédérale, toutes les affaires courantes de la DSK étaient *de facto* gérées par un fonctionnaire fédéral, qui restait lié par les instructions et la supervision du Gouvernement Fédéral. La Commission a par ailleurs déclaré qu'en étant structurellement intégrée aux autres services du Gouvernement Fédéral, la DSK n'était indépendante ni sur le plan organique ni sur le plan matériel. Tous les agents du bureau de la DSK étaient placés sous l'autorité de la chancellerie fédérale et, par conséquent, soumis à la tutelle de service de celle-ci. Enfin, la Commission a fait référence à une disposition du droit autrichien prévoyant le droit à l'information du chancelier fédéral.

La Cour a noté que l'article 28, paragraphe 1, de la directive 95/46 imposait aux États membres d'instituer une ou plusieurs autorités de contrôle qui exercent en toute indépendance leurs fonctions, pour la protection des données à caractère personnel, et que cette exigence résulte également du droit primaire de l'Union européenne, à savoir sa Charte des droits fondamentaux.

La Cour a rejeté l'argument selon lequel la DSK bénéficiait du degré d'indépendance requis par la directive dès lors qu'elle satisfaisait déjà à la condition d'indépendance pour pouvoir être qualifiée de juridiction d'un État membre, et a jugé que l'expression « en toute indépendance » de la directive devait recevoir une interprétation autonome et, notamment, que les autorités de contrôle de la protection des données à caractère personnel devaient jouir d'une indépendance qui leur permette d'exercer leurs missions sans influence extérieure, qu'elle soit directe ou indirecte, qui serait susceptible d'orienter leurs décisions.

La Cour a jugé que, indépendamment de l'autorité fédérale à laquelle le membre administrateur de la DSK appartenait, il existait un lien de service entre le membre administrateur et l'autorité fédérale, qui

permettait au supérieur hiérarchique dudit membre administrateur de contrôler les activités de ce dernier. Le supérieur hiérarchique jouit en effet d'un pouvoir de contrôle étendu sur les fonctionnaire de son département, qui lui permet non seulement de veiller à ce que ses collaborateurs s'acquittent des tâches qui leur incombent dans le respect des lois et d'une manière efficace et économe, mais également de les guider dans l'exercice de leurs fonctions, de remédier aux éventuelles fautes ou carences, de veiller au respect du temps de travail, de favoriser leur avancement en fonction de leurs performances, et de les orienter vers les tâches correspondant le mieux à leurs capacités.

Même si la loi autrichienne vise à empêcher le supérieur hiérarchique du membre administrateur de la DSK de donner des instructions à ce dernier, le fait est que cette loi octroie au supérieur hiérarchique un pouvoir de contrôle susceptible d'entraver l'indépendance de la DSK dans l'exercice de ses missions.

Sur le second grief, la Cour a observé que, bien que la DSK n'ait pas besoin d'une ligne budgétaire autonome pour pouvoir satisfaire au critère d'indépendance, l'attribution des moyens humains et matériels nécessaires à ces autorités ne devait pas l'empêcher d'exercer ses missions « en toute indépendance ». Or, le personnel mis à la disposition du bureau de la DSK était composé de fonctionnaires de la chancellerie fédérale soumis au contrôle de celle-ci, ce qui n'était pas compatible avec l'exigence d'indépendance.

Le fait que la DSK soit composée de fonctionnaires de la chancellerie fédérale, elle-même soumise au contrôle de la DSK, représentait un risque d'influence sur les décisions de la DSK. Une telle imbrication organisationnelle entre la DSK et la chancellerie fédérale empêchait que la DSK fût au-dessus de tout soupçon de partialité et était dès lors incompatible avec l'exigence d'« indépendance ».

Enfin, la Cour a jugé que le droit du chancelier fédéral à être informé à tout moment par le président et le membre administrateur de tous les aspects liés au travail de la DSK était susceptible de soumettre la DSK à l'influence indirecte du chancelier fédéral, ce qui était incompatible avec le critère d'indépendance, et s'opposait à ce que la DSK puisse être considérée comme pouvant opérer, en toutes circonstances, au-dessus de tout soupçon de partialité.

La Cour a jugé qu'en ne prenant pas toutes les dispositions nécessaires pour que la législation en vigueur en Autriche satisfasse au critère d'indépendance concernant la Datenschutzkommission (commission de protection des données), plus précisément, en instituant un cadre réglementaire en vertu duquel le membre administrateur de la Datenschutzkommission est un fonctionnaire fédéral assujetti à une tutelle de service, le bureau de la Datenschutzkommission est intégré aux services de la chancellerie fédérale, et le chancelier fédéral dispose d'un droit inconditionnel à l'information sur tous les aspects de la gestion de la Datenschutzkommission, la République d'Autriche a manqué aux obligations qui lui incombent en vertu de l'article 28, paragraphe 1, second alinéa, de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

3.3. CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

A : Résumé des activités et actualités :

Au cours de l'année 2012, le CEPD a une fois encore fixé de nouveaux points de référence dans différents domaines d'activité. En matière de supervision des institutions et organes européens dans le cadre du traitement de données à caractère personnel, le CEPD a interagi avec un plus grand nombre de délégués à la protection des données dans un plus grand nombre d'institutions et d'organismes que jamais auparavant. Par ailleurs, le CEPD a observé les effets de sa nouvelle politique d'application : la plupart des institutions et organes de l'UE, y compris de nombreuses agences, progressent bien dans leur respect du règlement sur la protection des données, tandis que d'autres devraient encore intensifier leurs efforts.

Lors de la consultation sur les nouvelles mesures législatives, le CEPD a émis un nombre record d'avis sur différents sujets. L'examen du cadre juridique européen pour la protection des données était l'un des premiers points à l'ordre du jour du CEPD. Toutefois, la mise en œuvre du programme de Stockholm dans les domaines de la liberté, de la sécurité et de la justice et de l'Agenda numérique, ainsi que des questions de marché intérieur, telles que la réforme du secteur financier, ou encore de santé publique et d'affaires des consommateurs, ont également eu un impact sur la protection des données. Le CEPD a également intensifié sa coopération avec les autres autorités de contrôle.

Des efforts particuliers ont été consacrés à l'amélioration de l'efficacité de l'organisation du CEPD en ces temps d'austérité. Dans ce contexte, le CEPD a procédé à un examen stratégique approfondi, dont découlent des objectifs pour 2013-14 et un règlement intérieur couvrant l'ensemble des activités du CEPD et l'adoption d'un plan de gestion annuel.

Organisation	Contrôleur européen de la protection des données (CEPD)
Président et/ou collège	Peter Hustinx, Contrôleur Giovanni Buttarelli, Contrôleur adjoint
Budget	7 624 090 EUR
Personnel	58 (toutes catégories de personnel incluses)
Activités générales	
Décisions, avis, recommandations	33 avis législatifs portant, notamment, sur les initiatives liées aux domaines de la liberté, de la sécurité et de la justice, aux développements technologiques, à la coopération internationale, aux transferts de données et au marché interne. 15 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 ». 37 séries d'observations informelles

Notifications	119 notifications d'opérations de traitement reçues de la part de délégués à la protection des données auprès des institutions et organes de l'UE à des fins d'examen préalable
Examens préalables	71 avis de contrôle préalable adoptés concernant, notamment, les données de santé, l'évaluation du personnel, le recrutement, les suspicions et les délits, et la surveillance en ligne. 11 avis sur l'absence de contrôle préalable adoptés.
Demandes émanant des personnes concernées	116 demandes d'informations et de conseils reçues du public ou de parties intéressées comprenant des demandes sur la législation européenne en matière de protection des données et son examen, l'informatique en nuage, l'ACAC, la santé en ligne, les cookies et la vie privée en ligne, les données biométriques, le consentement, les systèmes d'information à grande échelle tels que SIS et EURODAC et les questions de protection des données au sein de l'administration européenne telles que les activités de traitement par les institutions, organes et agences de l'UE.
Plaintes émanant des personnes concernées	86 plaintes reçues, dont 40 recevables Les principaux types de violations alléguées : droits d'accès et de rectification des données, d'objection et de suppression, collecte excessive de données, transfert de données, qualité des données et information des personnes concernées, sécurité des données ou divulgation de données.
Conseils sollicités par le Parlement ou le gouvernement	La plupart des 33 avis législatifs susmentionnés ont été exprimés à la demande de la Commission européenne (article 28, paragraphe 2, du règlement (CE) n° 45/2001).
Autres renseignements relatifs aux activités générales	27 consultations sur des mesures administratives liées au traitement de données à caractère personnel dans l'administration de l'UE. Des conseils ont été prodigués sur de nombreux aspects juridiques liés au traitement des données à caractère personnel par les institutions et les organes de l'UE.
Activités d'inspection	
Contrôles, enquêtes	15 contrôles sur place et 6 visites réalisés.
Activités de sanction	s. o.
DPD	
Chiffres relatifs aux DPD	58 DPD au sein des institutions, organes et agences de l'UE.

B. Informations sur la jurisprudence

Participation du CEPD aux poursuites judiciaires

En 2012, le CEPD est intervenu dans quatre affaires devant la Cour de Justice de l'UE et le Tribunal de la fonction publique.

La première affaire portait sur l'absence alléguée d'indépendance de l'autorité autrichienne de protection des données (DSK). Le CEPD a soutenu la position de la Commission qui arguait que l'indépendance fonctionnelle de la DSK prévue par la loi autrichienne n'était pas suffisante. La Cour a suivi ce raisonnement et conclu que ses liens étroits avec la chancellerie fédérale autrichienne empêchaient la DSK d'être au-dessus de tout soupçon de partialité.

La deuxième affaire dans laquelle le CEPD est intervenu au bénéfice du demandeur était *Egan et Hackett / Parlement européen* (Affaire T-190/10). Il s'agissait de la dernière de trois affaires pour lesquelles la Cour générale a dû se prononcer sur la relation entre le règlement concernant l'accès public aux documents et le règlement sur la protection des données après la décision déterminante prise dans l'affaire *Bavarian Lager / Commission* du 29 juin 2010 (Affaire C-28/08 P). Comme dans les deux autres affaires, le CEPD a argumenté en faveur d'une plus grande transparence.

Le CEPD est intervenu dans deux autres affaires toujours en cours d'instruction au moment de la rédaction du présent rapport. La première affaire concerne une procédure d'infraction contre la Hongrie sur l'indépendance de l'autorité de protection des données. La seconde, devant le Tribunal de la fonction publique, concerne une violation alléguée du règlement de l'UE sur la protection des données (CE) n° 45/2001 dans le cadre d'une enquête interne sur une plainte de harcèlement par la BEI.

Le CEPD a également suivi de près plusieurs autres affaires sans intervenir, telles que l'affaire de Google Espagne qui porte principalement sur l'applicabilité de la loi espagnole mettant en application la directive européenne sur la protection des données à l'égard des activités de Google, et deux autres affaires liées à la validité de la directive européenne sur la conservation des données.

C. Autres informations importantes

Examen du cadre européen de protection des données

En 2012, le principal projet législatif du CEPD était sans nul doute le paquet de réformes sur la protection des données. Le CEPD a souligné la nécessité d'actualiser et de renforcer les règles de l'UE sur la protection des données en de nombreuses occasions et, le 25 janvier, la Commission a adopté son programme de réformes, comprenant deux propositions législatives : un règlement général sur la protection des données et une directive spécifique sur la protection des données dans les domaines de la police et de la justice.

La première réaction du CEPD a été de saluer le règlement général comme représentant un grand pas en avant pour la protection des données en Europe, un excellent point de départ pour l'adoption de règles européennes sur la protection des données qui soient suffisamment robustes pour faire face aux futurs défis liés aux technologies de l'information.

Concernant la directive, toutefois, le CEPD a été très critique vis-à-vis de son contenu inadéquat. Il a souligné le fait que la Commission n'avait pas respecté ses promesses visant à garantir un système robuste pour la protection des données dans les domaines de la police et de la justice et s'est demandé pourquoi la Commission avait exclu ces domaines de ce qu'elle comptait faire initialement, à savoir proposer un cadre législatif global.

Le 7 mars, le CEPD a adopté un avis développant plus en détails sa position sur ces deux propositions. Dans une déclaration publique, le CEPD a conclu que ces deux propositions législatives ne contribueraient pas à rapprocher l'Europe d'un ensemble global de règles en matière de protection des données et ce, tant sur le plan national qu'européen, dans tous les domaines de la politique européenne. Ceci est d'autant plus vrai que les propositions ne produisent aucun effet sur de nombreux instruments existants de l'UE en matière de protection des données, tels que les règles de protection des données pour les institutions et organes de l'UE, mais aussi les instruments spécifiques adoptés dans le domaine de la police et de la justice.

Le CEPD a néanmoins salué une amélioration spécifique de la directive proposée, à savoir le fait que la proposition couvre également la question du traitement national. Le CEPD a toutefois souligné que cette amélioration n'offrirait de plus-value que si la directive renforçait substantiellement le niveau de protection des données dans ce domaine, ce qui n'est pas le cas.

Le CEPD a également observé que les règles de protection des données proposées en matière d'application des lois étaient d'une faiblesse inacceptable. Il a noté de nombreux exemples d'écarts injustifiés par rapport aux règles prévues dans la proposition de règlement. Il a en outre précisé que des règles spécifiques étaient nécessaires dans le domaine répressif, et non une baisse généralisée du niveau de protection des données.

Le CEPD a également exprimé des inquiétudes particulières portant sur :

- l'absence de sécurité juridique quant à l'utilisation ultérieure des données à caractère personnel par les autorités répressives ;
- l'absence d'une obligation générale pour les autorités répressives de démontrer la conformité avec les exigences de protection des données ;
- les conditions insuffisantes pour les transferts vers des pays tiers ;
- les pouvoirs indûment limités des autorités de contrôle.

Tout au long de l'année, le CEPD a fait plusieurs discours précisant sa position sur le paquet de réformes et a participé à des discussions thématiques. Il est resté à la disposition du législateur européen pour de plus amples conseils ou explications sur notre position. En outre, de par sa participation au groupe de travail « Article 29 », le CEPD a donné des informations sur plusieurs sujets plus spécifiques.

Le CEPD s'est également efforcé d'encourager de plus amples discussions. En septembre et novembre, en étroite coopération avec la Europäische Rechtsakademie (ERA), le CEPD a organisé deux séminaires consacrés à ces propositions. Les séminaires ont rassemblé de nombreux experts des administrations nationales, des autorités de protection des données, des institutions européennes, du monde universitaire, des pays tiers et du secteur privé. Le CEPD a également lancé une page web consacrée au processus de réforme contenant toute la documentation pertinente, accessible via un lien sur son site Internet.

Chapitre Quatre

Principaux développements dans les pays de l'EEE

ISLANDE

A. Résumé des activités et actualités :

Début 2012, la Direction nationale de la santé a demandé des informations aux chirurgiens plastiques sur toutes les femmes qui se sont fait poser des implants mammaires depuis le début de l'année 2000. La raison en était la révélation de violations de la loi lors de la fabrication d'une marque de prothèses mammaires appelée PIP. Le syndicat des médecins islandais, qui était opposé à l'idée de fournir les informations demandées, a cherché conseil auprès de la DPA afin de déterminer s'il était légal de communiquer à la Direction nationale de la santé des informations personnelles sur les personnes concernées, y compris leurs diagnostics et identités. Cette collecte de données planifiée par la Direction avait pour objet, notamment, de pouvoir s'adresser aux femmes ayant des implants mammaires PIP, de savoir si elles se rendaient à des visites régulières de dépistage du cancer du sein et de comparer les différences statistiques entre la santé des femmes portant des prothèses mammaires PIP et celle des femmes ayant d'autres types d'implants mammaires. D'après le syndicat des médecins islandais, toutefois, de nombreuses femmes avaient exprimé leur inquiétude quant à la communication de leurs informations. Par ailleurs, le syndicat a déclaré que les femmes ayant des implants mammaires PIP avaient déjà reçu, de la part du chirurgien plastique concerné, un courrier soulevant ce problème. La DPA a donné des conseils dans le cadre de deux avis distincts, l'un en avril concernant les données de femmes ayant des implants PIP et le second en mars concernant les femmes ayant d'autres types d'implants. La conclusion de ces deux avis a été que la Direction nationale de la santé ne jouissait pas de la compétence juridique nécessaire pour demander ces informations et, par conséquent, que les chirurgiens plastiques n'étaient pas autorisés à les communiquer sans le consentement des personnes concernées.

En 2012, une autre affaire notable a porté sur la diffusion de données à caractère personnel de personnes en détresse financière par le Médiateur des débiteurs. Le Médiateur représente les intérêts des débiteurs, en partie en facilitant la conclusion d'accords de réduction de leurs dettes avec leurs créanciers. Dans le cadre de ce travail, le Médiateur a envoyé un courriel à quatre fonds de pension, tous créanciers de prêts immobiliers, et (par erreur) à l'hôpital national. Une liste de près de 3 000 clients du Médiateur était jointe à ce courriel. Cette liste était transmise afin de demander aux fonds de pension si les personnes de la liste avaient bénéficié de quelque mesure de réduction de leurs dettes. L'un des fonds de pension s'est alarmé de cette transmission de données et a alerté la DPA, qui a enquêté. La DPA a conclu que le bureau du Médiateur était légalement habilité à demander si ses clients avaient bénéficié de la mesure en question. La DPA a néanmoins souligné que, dans le cadre de la collecte d'informations, le bureau du Médiateur n'était pas légalement autorisé à transmettre des listes exhaustives de personnes ayant demandé son assistance, uniquement parce que les destinataires de cette liste étaient susceptibles de détenir des informations pertinentes sur certaines de ces personnes. Par conséquent, la DPA a conclu que la transmission de cette liste constituait une violation de la loi sur la protection des données. La DPA a par ailleurs ordonné au bureau du Médiateur de fournir un descriptif écrit de son système de gestion de la sécurité du traitement des données à caractère personnel.

Organisation	Autorité de protection des données
Président et/ou collège	Mme Sigrún Jóhannesdóttir, Commissaire ; Mme Björg Thorarensen, Présidente du Conseil d'administration.
Budget	60 176 567 ISK (équivalent à 353 418 EUR au taux de change officiel du 31 décembre 2012).

Personnel	Cinq avocats, un secrétaire.
Activités générales	
Décisions, avis, recommandations	150 (environ)
Notifications	551
Examens préalables	133 autorisations de traitement ont été accordées.
Demandes émanant des personnes concernées	500 (environ)
Plaintes émanant des personnes concernées	111
Conseils sollicités par le Parlement ou le gouvernement	50 (environ)
Autres renseignements relatifs aux activités générales	Au total, 1 489 nouvelles affaires ont été enregistrées en 2012.
Activités d'inspection	
Contrôles, enquêtes	3
Activités de sanction	
Sanctions	À l'exception des amendes journalières émises pour chaque jour où ses décisions ne sont pas appliquées, la DPA ne possède aucun pouvoir de sanction. Aucune amende journalière n'a été imposée en 2011.
Amendes	À l'exception des amendes journalières émises pour chaque jour où ses décisions ne sont pas appliquées, la DPA ne possède aucun pouvoir de sanction. Aucune amende journalière n'a été imposée en 2011.
DPD	
Chiffres relatifs aux DPD	s. o.

B. Informations sur la jurisprudence

Le 27 août 2012, dans le cadre de l'affaire 562/2012, la Cour Suprême d'Islande a infirmé une ordonnance émise en première instance, en vertu de laquelle les fournisseurs de téléphones sans fil proposant leurs services sur les îles Vestmann avaient l'obligation de communiquer à la police des informations sur tous les appels entrants et sortants passés par des tours de téléphonie cellulaire spécifiques dans un intervalle de 10 minutes le matin du 6 août 2012. Cette ordonnance avait été émise en relation avec une enquête policière sur une agression sexuelle présumée avoir été perpétrée

pendant ce laps de temps près des tours de téléphonie cellulaire en question. À cette époque, un suspect avait été observé, sur l'enregistrement d'un système de vidéosurveillance, fuyant la scène tout en parlant au téléphone. L'article 80 de la loi relative à la procédure pénale prévoit que la police soit autorisée à demander aux entreprises de télécommunications des informations « sur les appels téléphoniques ou autres télécommunications d'un téléphone, ordinateur ou autre appareil de télécommunication spécifique ». La Cour Suprême a jugé que, dans la mesure où cette disposition constitue une exception au droit à la vie privée prévu par l'article 71 de la Constitution, il ne saurait être interprété plus largement que ce que prévoit littéralement le texte. Par conséquent, étant donné que l'ordonnance du tribunal n'identifie pas des informations concernant un téléphone spécifique, cette ordonnance se devait d'être infirmée.

LIECHTENSTEIN

A. Résumé des activités et actualités

En 2012, la loi sur la protection des données (DSG) est entrée en vigueur pour une durée de dix ans. Pour marquer cet événement, une enquête représentative parmi la population a été commanditée, basée sur l'Eurobaromètre 225 de 2008. Pour résumer, les conclusions suivantes ont pu être tirées : les citoyens affichent une grande confiance dans les établissements publics en général, et en la législation en particulier. Toutefois, ce constat est qualifié par le fait que 70 % de la population déclare n'avoir que peu de connaissances en matière de protection des données. Du point de vue du bureau de protection des données (Datenschutzstelle, DSS), l'enquête montre que les gens devraient être mieux informés. Sans surprise, cette enquête montre également que les jeunes sont mal informés et que, bien que les personnes aient connaissance de leurs droits, celles qui connaissent leur droit à l'information sont moins nombreuses que celles qui connaissent les droits de suppression ou de correction. Ce constat est paradoxal, dans la mesure où le droit de suppression ne peut être revendiqué que si la personne sait quelles données sont traitées, une information qui ne peut être trouvée que grâce au droit à l'information. Le plus remarquable, selon nous, réside dans le fait que seulement 40 % des personnes savaient qu'il existe un droit général d'indemnisation, et que 42 % pensaient qu'il n'en existait aucun. La directive générale 95/46/CE relative à la protection des données prévoit ce droit, qui s'applique bien qu'il n'ait pas été intégré à la DSG du Liechtenstein. Enfin, environ 28 % des personnes interrogées ont déclaré savoir qu'il existait une autorité de protection des données indépendante. Sur ces 28 %, seuls 15 % ont affirmé avoir déjà été en contact avec celle-ci. Ces chiffres peuvent peut-être s'expliquer par le haut niveau de confiance susmentionné, qui impliquerait qu'il n'y ait aucune raison de la contacter ; une autre raison pourrait être plus simplement un niveau de connaissance insuffisant et la non identification d'un problème possible ; la troisième raison possible pourrait être liée à l'ignorance de la possibilité d'indemnisation. Pour de plus amples détails, se reporter au Rapport d'activité 2012.

Une modification de la DSG est entrée en vigueur début octobre. Cette modification a pour principal objet la transposition de la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale. Par conséquent, la restriction de l'application de la DSG aux procédures pénales pendantes a été supprimée, et les dispositions relatives à la protection des données ont été intégrées au Code de procédure pénale. En outre, la disposition sur l'information préalable a été renforcée et amendée afin de refléter la directive 95/46/CE. Sur demande de l'autorité de surveillance de l'AELE, la disposition relative à l'obligation des sociétés de notifier les ensembles de données a été renforcée.

Un événement public a de nouveau été organisé avec l'Université du Liechtenstein à l'occasion de la Journée européenne de la protection des données. Le thème de l'événement était le suivant : « Que sait l'Internet sur moi ? Mes données en tant que bien commercialisable ». La question du ciblage en ligne a été examinée.

Dans la société actuelle, l'anonymisation est une mesure importante pour protéger les données à caractère personnel. La pseudonymisation revêt également une grande importance. Des lignes directrices ont été élaborées et publiées sur ces deux sujets.

Organisation	Bureau de la protection des données
Président et/ou collège	Philipp Mittelberger
Budget	596 000 EUR

Personnel	2,3 ETP Droit ; 1,0 ETP Technologie ; 0,8 ETP Administration
Activités générales	
Décisions, avis, recommandations	9 Réponses à des projets de loi ([17]) 4 Autorisations relatives à des systèmes de vidéosurveillance
Notifications	À la fin de l'année, 384 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).
Examens préalables	s. o.
Demandes émanant des personnes concernées	89 demandes émanant de particuliers
Plaintes émanant des personnes concernées	s. o.
Conseils sollicités par le Parlement ou le gouvernement	Aucun
Autres renseignements relatifs aux activités générales	640 demandes ([18]) (de particuliers inclus, voir ci-dessus)
Activités d'inspection	
Contrôles, enquêtes	3 contrôles réalisés
Activités de sanction	
Sanctions	s. o.
Amendes	s. o.
DPD	
Chiffres relatifs aux DPD	50 délégués à la protection des données

B. Informations sur la jurisprudence

Rien à mentionner.

([17]) Cf. Rapport d'activité 2012 du Bureau de protection des données, sous le n° 3, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2012.pdf.

([18]) Voir les statistiques sur les demandes du Bureau de la protection des données, sous le n° 8.1., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2012.pdf.

NORVÈGE

A. Résumé des activités et actualités

Nouvelles stratégies

Conformément à la stratégie déployée dans le secteur de la santé, nous avons continué de développer des stratégies pour les secteurs de la justice et de la police et pour notre engagement international. Nous avons en outre accordé une plus grande attention à la manière dont nous mettons en œuvre nos procédures administratives et de contrôle.

En 2012, nous avons augmenté le nombre d'audits de 20 pour cent, amélioré la gestion des affaires individuelles et professionnalisé nos services de conseils.

Séquelles de l'attaque du 22 juillet 2011

Lors de l'examen de plusieurs propositions de mesures législatives du ministère de la Justice, qui s'est avéré être un exercice houleux et justifié, nous avons noté que nous devions garder la tête froide après les événements tragiques du 22 juillet 2011. Il a également été important pour nous de souligner que la DPA souhaite faire partie de l'équipe qui résoudra les futurs défis grâce à ses connaissances des nouvelles technologies et du développement communautaire.

Nouveau site web

L'une des principales priorités stratégiques consiste à permettre à chaque citoyen de sauvegarder sa vie privée. L'une des principales mesures mises en œuvre dans cet objectif a été le lancement de notre nouveau site web. Sa conception repose sur une philosophie d'entraide et de partage des bonnes informations avec les citoyens et les responsables du traitement des données.

Organisation	Autorité norvégienne de protection des données
Président et/ou collège	Directeur Bjørn Erik Thon
Budget	36 millions de NOK
Personnel	41
Activités générales	
Décisions, avis, recommandations	
Notifications	2 954 nouvelles notifications enregistrées, 10 909 actives au total. (À la fin de l'année, il nous restait encore plus de 2 000 notifications à enregistrer, ce nombre de nouvelles notifications devrait donc être plus élevé.)
Examens préalables	132
Demandes émanant des	Au total, la DPA norvégienne a reçu 4 675 appels téléphoniques et

personnes concernées	2 175 courriels adressés à nos services de conseils.
Plaintes émanant des personnes concernées	s. o.
Conseils sollicités par le Parlement ou le gouvernement	Nous avons reçu 105 invitations à commenter la nouvelle législation et envoyé des commentaires à 58 occasions.
Autres renseignements relatifs aux activités générales	
Activités d'inspection	
Contrôles, enquêtes	Télécommunications, Internet et DLD - 7 Lieu de travail - 10 Secteur financier - 6 Secteur de la santé- 5 Justice et police - 2 Secteur public - 13 Caméras - 4 Sécurité des informations - 4 Deuxièmes audits - 4 Total - 55
Activités de sanction	
Sanctions	7 amendes et 2 amendes coercitives, toutes imposées par la DPA
Amendes	Total des amendes : 1 300 000 NOK, amendes coercitives : 49 000 NOK
DPD	
Chiffres relatifs aux DPD	203 DPD représentant 390 sociétés et bureaux publics au total.

B. Informations sur la jurisprudence

Nous avons rendu nombre de jugements différents en 2012, et nous n'en présenterons ici que quelques-uns parmi les plus importants.

Affaire GE — divulgation non autorisée d'informations sur la santé

La DPA a eu connaissance, en mars 2012, de la divulgation non autorisée d'informations sur la santé par plusieurs entreprises (responsables du traitement de données) au fournisseur GE Healthcare Systems (GE) aux États-Unis. Nous soupçonnons que des informations concernant un nombre substantiel de patients, dont leur nom, leur numéro d'identité, leur date de naissance et leurs données de santé, ont été récupérées et transférées à GE. Cette indiscrétion était imputable à onze entreprises norvégiennes. Les informations initiales établissaient que les informations de 126 344 patients étaient concernées, mais ce chiffre est incertain.

Les hôpitaux en question avaient un accord avec le fournisseur GE concernant l'exploitation, l'entretien et la supervision de matériel. La connexion avait été configurée de telle manière que GE pouvait récupérer les informations sur la santé sans avoir aucun obstacle à franchir.

Dans notre jugement, nous avons déclaré que les responsables du traitement de données devaient établir des garanties appropriées pour assurer la confidentialité, et que les patients affectés devaient être informés de l'incident.

L'affaire Nettby

La DPA a décidé en 2011 la suppression des informations personnelles issues du réseau social Nettby désormais fermé (propriété du journal VG, l'un des tabloïds les plus influents de Norvège). VG a contesté la décision et c'est la commission de recours en matière de vie privée qui a jugé l'affaire. Celle-ci a déclaré qu'il était obligatoire de déposer à la Bibliothèque Nationale certains des « documents » (ou informations) que VG souhaitait conserver, tels que les contenus de forums ouverts et les parties susceptibles d'être indexées dans les moteurs de recherche. La décision est également applicable aux informations qui ne devaient pas être indexées mais étaient mises à disposition de tous les membres de Nettby. VG devait respecter cette obligation légale avant d'effacer les informations.

Cette décision est importante si l'on considère le nombre de personnes qui utilisent les sites de réseaux sociaux. Le public pense probablement qu'il peut décider, dans une certaine mesure, de la durée de stockage des informations et des personnes autorisées à y avoir accès, que ce soit sur l'instant présent ou à l'avenir.

La commission de recours a conclu que toute personne mettant une plateforme telle que Nettby à disposition du public était tenue de déposer des « documents » à la Bibliothèque Nationale.

C. Autres informations importantes

Rapport sur la cybersurveillance sur le lieu de travail

En 2012, la DPA a préparé un rapport intitulé « Une journée normale au travail — la cybersurveillance sur le lieu de travail ». Ce rapport avait pour objet d'illustrer la manière dont les informations personnelles sont collectées et utilisées dans la vie professionnelle de tous les jours, ainsi que d'informer et de sensibiliser. Dans ce rapport, nous avons considéré la journée de travail de trois professions différentes : conducteur de bus, infirmière à domicile et gestionnaire de dossiers. Nous avons organisé des entrevues avec des représentants de la direction et des employés des trois groupes professionnels sélectionnés.

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 2012

Allemagne	Autriche
M. Peter Schaar Commissaire fédéral à la protection des données et au droit à l'information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) Husarenstraße 30 - DE -53117 Bonn Tél. : +49 (0) 228 99-7799-0 Fax : +49 (0) 228 99-7799-550 Adresse électronique : poststelle@bfdi.bund.de Site web : http://www.datenschutz.bund.de M. Alexander Dix (représentant les états allemands / Bundesländer) Commissaire du Land 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 Wien Tél. : +43 1 531 15 / 202525 Fax : +43 1 531 15 /202690 Adresse électronique : dsk@dsk.gv.at Site web : http://www.dsb.gv.at/
Belgique	**Bulgarie**
M. Willem Debeuckelaere Commission de la protection de la vie privée (Commission for the protection of privacy / Commissie voor de bescherming van de persoonlijke levenssfeer) Rue de la Presse, 35 -1000 Bruxelles Tél. : +32(0)2/274 48 00 Fax : +32(0)2/274 48 35 Adresse électronique : commission@privacycommission.be	M. Krassimir Dimitrov Commission de protection des données à caractère personnel – CPDP (Комисия за защита на личните данни) 15, Acad.Ivan Evstratiev Geshov blvd. BG- 1431 Sofia Tél. : +359 2 915 3501 Fax : +359 2 915 3525 Adresse électronique : kzld@government.bg, kzld@cpdp.bg

Site web : http://www.privacycommission.be/	Site web : http://www.cpdp.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, 2nd floor - CY - 1082 Nicosia (P.O. Box 23378 - CY - 1682 Nicosia) Tél. : +357 22 818 456 Fax : +357 22 304 565 Adresse électronique : commissioner@dataprotection.gov.cy Site web : http://www.dataprotection.gov.cy	Mme Janni Christoffersen Agence danoise de protection des données (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tél. : +45 3319 3200 Fax : +45 3319 3218 Adresse électronique : dt@datatilsynet.dk Site web : http://www.datatilsynet.dk
Espagne	**Estonie**
M. José Luis Rodriguez Álvarez Agence espagnole de protection des données (Agencia Española de Protección de Datos) 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 Inspection estonienne de la protection des données (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, 6rd floor - FI - 00251 Helsinki (P.O. Box 800) Tél. : +358 295 666 700	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

Fax : +358 295 666 735 Adresse électronique : tietosuoja@om.fi Site web : http://www.tietosuoja.fi	Tél. : +33 1 53 73 22 22 Fax : +33 1 53 73 22 00 Adresse électronique : lfalquepierrotin@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 – Grèce Tél. : +30 210 6475608 Fax : +30 210 6475789 Adresse électronique : p.christoforos@dpa.gr Site web : http://www.dpa.gr	Dr Attila Péterfalvi Président Autorité nationale pour la protection des données et la liberté d'information de Hongrie (Nemzeti Adatvédelmi és Információszabadság Hatóság) Szilágyi Erzsébet fasor 22/c - HU - 1125 Budapest Tél. :+36 1 391 1400 Fax : +36 1 391 1410 Adresse électronique : ugyfelszolgalat@naih.hu Site web : 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 Roma 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 Inspection nationale des données de Lettonie (Datu valsts inspekcija) Blaumana street 11/13-15 Riga, LV-1011 Lettonie Tél. : + 371 67223131	M. Algirdas Kunčinas 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

Fax : + 371 67223556 Adresse électronique : info@dvi.gov.lv Site web : www.dvi.gov.lv	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 Malte 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 : http://www.cbpweb.nl http://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 Warsaw Tél. : +48 22 860 7312 ; +48 22 860 70 81 Fax : +48 22 860 73 13 Adresse électronique : desiwm@giodo.gov.pl Site web : http://www.giodo.gov.pl
Portugal	**République tchèque**
Mme Filipa Calvão Commission nationale de protection des données (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º	M. Igor Nemec Bureau de la protection des données à caractère personnel (Úřad pro ochranu osobních údajů)

PT - 1 200-821 Lisboa Tél. : +351 21 392 84 00 Fax : +351 21 397 68 32 Adresse électronique : geral@cnpd.pt Site web : http://www.cnpd.pt	Pplk. Sochora 27 - CZ - 170 00 Praha 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 Georgeta Basarabescu Autorité nationale de contrôle du traitement des données à caractère personnel (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Bd. Gral. Ghe. Magheru 28-30, 5th floor, room 5, 1st district, postal code 010336, RO - Bucharest Tél. : +40 31 805 9211 Fax : +40 31 805 9602 Adresse électronique : international@dataprotection.ro ; anspdcp@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. : +44 1625 545700 Fax : +44 1625 524510 Adresse électronique : veuillez compléter le formulaire de demande sur notre site web Site web : 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 2 323 132 11 Fax : +421 2 323 132 34 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 (Datainspektionen)	M. Peter Hustinx Contrôleur européen de la protection des données — CEPD

Drottninggatan 29, 5th floor 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 : rue Montoyer, 30, BE - 1000 Bruxelles Tél. : +32 2 283 1915 Fax : +32 2 283 1950 Adresse électronique : edps@edps.europa.eu Site web : www.edps.europa.eu

OBSERVATEURS DU GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES EN 2012

Islande	Norvège
Mme Sigrun Johannesdottir Autorité de protection des données (Persónuvernd) Raudararstigur 10 - IS - 105 Reykjavik Tél. : +354 510 9600 Fax : +354 510 9606 Adresse électronique : postur@personuvernd.is Site web : http://www.personuvernd.is	M. Kim Ellertsen 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
Liechtenstein	**République de Croatie**
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	M. Dubravko Bilić Directeur Mme Sanja Vuk Chef du département des affaires juridiques et de l'UE 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 info@azop.hr Site web : http://www.azop.hr/default.asp

Ancienne République yougoslave de Macédoine	
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	

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

DS-AA-15-001-FR-N

doi:10.2838/202799