

# Rapport annuel

**2007**



LE CONTRÔLEUR EUROPÉEN  
DE LA PROTECTION DES DONNÉES





# Rapport annuel

## 2007



LE CONTRÔLEUR EUROPÉEN  
DE LA PROTECTION DES DONNÉES

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**

(\* Certains opérateurs de téléphonie mobile ne permettent pas l'accès aux numéros 00 800 ou peuvent facturer ces appels.

De nombreuses autres informations sur l'Union européenne sont disponibles sur l'internet  
via le serveur Europa (<http://europa.eu>).

Une fiche bibliographique figure à la fin de l'ouvrage.

Luxembourg: Office des publications officielles des Communautés européennes, 2008

ISBN 978-92-95030-42-8

© Photos: Parlement européen et iStockphoto

© Communautés européennes, 2008

Reproduction autorisée, moyennant mention de la source

*Printed in Italy*

IMPRIMÉ SUR PAPIER BLANCHI SANS CHLORE

# Table des matières

Guide de l'utilisateur	6
Mandat	7
Avant-propos	8
1. Bilan et perspectives	9
1.1. Aperçu général de 2007	9
1.2. Résultats obtenus en 2007	10
1.3. Objectifs en 2008	11
2. Supervision	12
2.1. Introduction	12
2.2. Délégués à la protection des données	12
2.3. Contrôles préalables	14
2.3.1. Base juridique	14
2.3.2. Procédure	14
2.3.3. Analyse quantitative	16
2.3.4. Principales questions soulevées par les cas examinés a posteriori	20
2.3.5. Principales questions soulevées dans le cadre des contrôles préalables proprement dits	22
2.3.6. Consultations quant à la nécessité d'un contrôle préalable	24
2.3.7. Notifications non soumises au contrôle préalable	25
2.3.8. Suivi des avis relatifs aux contrôles préalables	26
2.3.9. Conclusions et perspectives	26
2.4. Plaintes	27
2.4.1. Introduction	27
2.4.2. Plaintes déclarées recevables	27
2.4.3. Plaintes déclarées irrecevables: principaux motifs d'irrecevabilité	30
2.4.4. Collaboration avec le Médiateur européen	30
2.4.5. Travaux complémentaires dans le domaine des plaintes	31
2.5. Enquêtes	31
2.6. Action en matière d'inspection	32
2.6.1. L'échéance du «printemps 2007» et au-delà	32
2.6.2. Délégués à la protection des données	33
2.6.3. Inventaire des traitements	33
2.6.4. Inventaire des dossiers de contrôle préalable	33
2.6.5. Poursuite de la mise en œuvre	34
2.6.6. Conclusions	34
2.7. Mesures administratives	34
2.8. Contrôle des communications électroniques	36
2.9. Vidéosurveillance	37
2.10. Eurodac	38
3. Consultation	40
3.1. Introduction	40
3.2. Cadre d'action et priorités	41

<b>3.3. Avis législatifs</b>	<b>43</b>
3.3.1. Observations d'ordre général	43
3.3.2. Les avis du CEPD	44
<b>3.4. Observations</b>	<b>49</b>
<b>3.5. Interventions devant la Cour de justice</b>	<b>51</b>
<b>3.6. Autres activités</b>	<b>51</b>
<b>3.7. Nouvelles évolutions</b>	<b>54</b>
3.7.1. Interaction avec la technologie	54
3.7.2. Faits nouveaux dans les domaines politique et législatif	55
<b>4. Coopération</b>	<b>57</b>
<b>4.1. Groupe de l'article 29</b>	<b>57</b>
<b>4.2. Groupe «Protection des données» du Conseil</b>	<b>58</b>
<b>4.3. Contrôle coordonné d'Eurodac</b>	<b>58</b>
<b>4.4. Troisième pilier</b>	<b>60</b>
<b>4.5. Conférence européenne</b>	<b>61</b>
<b>4.6. Conférence internationale</b>	<b>61</b>
<b>4.7. L'initiative de Londres</b>	<b>62</b>
<b>4.8. Organisations internationales</b>	<b>62</b>
<b>5. Communication</b>	<b>64</b>
<b>5.1. Introduction</b>	<b>64</b>
<b>5.2. Caractéristiques de la communication</b>	<b>64</b>
<b>5.3. Discours</b>	<b>65</b>
<b>5.4. Service de presse</b>	<b>67</b>
<b>5.5. Demandes d'informations ou de conseils</b>	<b>68</b>
<b>5.6. Outils d'information en ligne</b>	<b>69</b>
<b>5.7. Contacts avec les médias et visites d'étude</b>	<b>70</b>
<b>5.8. Événements promotionnels</b>	<b>70</b>
<b>6. Administration, budget et personnel</b>	<b>72</b>
<b>6.1. Introduction: développement de la nouvelle institution</b>	<b>72</b>
<b>6.2. Budget</b>	<b>72</b>
<b>6.3. Ressources humaines</b>	<b>74</b>
6.3.1. Recrutement	74
6.3.2. Programme de stages	74
6.3.3. Programme pour les experts nationaux détachés	74
6.3.4. Organigramme	74
6.3.5. Formation	75
<b>6.4. Assistance administrative et coopération interinstitutionnelle</b>	<b>75</b>
<b>6.5. Infrastructure</b>	<b>76</b>
<b>6.6. Environnement administratif</b>	<b>76</b>
6.6.1. Systèmes de contrôle et d'audit internes	76
6.6.2. Comité du personnel	76
6.6.3. Règlement intérieur	76
6.6.4. Délégué à la protection des données	77
6.6.5. Gestion des documents	77

<b>6.7. Relations extérieures</b>	<b>77</b>
<b>6.8. Objectifs pour 2008</b>	<b>77</b>
Annexe A — Cadre juridique	79
Annexe B — Extrait du règlement (CE) n° 45/2001	81
Annexe C — Liste des abréviations et acronymes	83
Annexe D — Liste des délégués à la protection des données	85
Annexe E — Délais de traitement des contrôles préalables par dossier et par institution	87
Annexe F — Liste des avis rendus à la suite d'un contrôle préalable	90
Annexe G — Liste des avis sur des propositions législatives	97
Annexe H — Composition du secrétariat du CEPD	99
Annexe I — Liste des accords et décisions administratifs	101

# Guide de l'utilisateur

Le lecteur trouvera à la suite de ce guide l'avant-propos de M. Peter Hustinx, le Contrôleur européen de la protection des données (CEPD), précédé de l'énoncé de ses missions.

Le **chapitre 1 («Bilan et perspectives»)** présente une vue générale des activités du CEPD. Il met également en lumière les résultats obtenus en 2007 et expose les principaux objectifs retenus pour 2008.

Le **chapitre 2 («Supervision»)** décrit de façon complète les travaux menés pour s'assurer que les institutions et organes de l'Union européenne (UE) s'acquittent de leurs obligations en matière de protection des données. La présentation générale est suivie d'une analyse du rôle des délégués à la protection des données (DPD) dans les administrations de l'UE. Ce chapitre comprend une analyse des contrôles préalables (quantité et contenu), des plaintes (y compris la collaboration avec le Médiateur européen), des enquêtes, de la politique d'inspection et des avis sur des mesures administratives traités en 2007. Il comprend aussi des parties consacrées au suivi électronique et à la vidéosurveillance, ainsi qu'une section qui fait le point sur la supervision d'Eurodac.

Le **chapitre 3 («Consultation»)** traite de l'évolution du rôle consultatif du CEPD. Il est axé sur les avis rendus sur des propositions législatives et documents connexes, ainsi que leur incidence dans un nombre croissant de domaines. Ce chapitre comporte également une analyse de thèmes horizontaux et présente des questions liées aux nouveautés technologiques. Il aborde en particulier les défis auxquels sera confronté le cadre actuel en matière de protection des données dans un avenir proche.

Le **chapitre 4 («Coopération»)** décrit le travail effectué dans des forums importants tels que le groupe de l'article 29, dans les autorités de contrôle communes relevant du troisième pilier, et lors de la conférence européenne et de la conférence internationale des commissaires à la protection des données.

Le **chapitre 5 («Communication»)** présente les activités d'information et de communication du CEPD et les résultats obtenus, ainsi que le travail du service de presse. Il passe également en revue l'utilisation de différents outils de communication, tels que le site internet, les bulletins d'information, le matériel d'information et les actions de sensibilisation.

Le **chapitre 6 («Administration, budget et personnel»)** détaille les principaux changements au sein de l'organisation du CEPD, notamment les aspects budgétaires, la question des ressources humaines et les accords de nature administrative.

Le rapport est complété par des **annexes** dans lesquelles figurent un aperçu du cadre juridique pertinent, les dispositions du règlement (CE) n° 45/2001, une liste d'abréviations et acronymes, des statistiques relatives aux contrôles préalables, la liste des DPD des institutions et organes de l'UE, ainsi que la description de la composition du secrétariat du CEPD et une liste des accords et décisions de nature administrative adoptés par le CEPD.

Une **synthèse** du présent rapport est également disponible, offrant une version abrégée des principaux faits intervenus en 2007 dans le cadre des activités du CEPD.

Pour de plus amples informations sur le CEPD, nous vous invitons à consulter notre site internet, qui reste notre principal outil de communication (<http://www.edps.europa.eu>). Le site internet permet également de s'inscrire en vue de recevoir notre bulletin d'information.

Il est possible de commander auprès des services du CEPD des exemplaires gratuits du rapport annuel et de la synthèse. Nos coordonnées sont indiquées sur notre site internet, sous la rubrique «Contact» <sup>(1)</sup>.

---

<sup>(1)</sup> <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/op/lang/fr/pid/46>.

## Mandat

Le Contrôleur européen de la protection des données (CEPD) a pour mission de veiller à ce que les institutions et organes de l'Union européenne, lorsqu'ils traitent des données à caractère personnel, respectent les droits fondamentaux et les libertés des personnes, en particulier leur vie privée. Le CEPD est chargé:

- de surveiller et d'assurer le respect des dispositions du règlement (CE) n° 45/2001, ainsi que d'autres actes communautaires concernant la protection des droits fondamentaux et des libertés lorsque les institutions et organes de l'UE traitent des données à caractère personnel («supervision»);
- de conseiller les institutions et organes de l'UE pour toutes les questions concernant le traitement de données à caractère personnel, ce qui inclut la consultation dans le cadre de l'élaboration de dispositions législatives, et le suivi des faits nouveaux ayant une incidence sur la protection des données à caractère personnel («consultation»);
- de coopérer avec les autorités nationales de contrôle et avec les organes de contrôle relevant du troisième pilier de l'UE, en vue d'améliorer la cohérence en matière de protection des données à caractère personnel («coopération»).

Conformément à ces lignes d'action, le CEPD a pour objectifs stratégiques:

- de promouvoir une culture de la protection des données au sein des institutions et organes, contribuant ainsi à améliorer la bonne gestion des affaires publiques;
- d'intégrer le respect des principes de protection des données dans la législation et la politique communautaires, le cas échéant;
- d'améliorer la qualité des politiques de l'UE, chaque fois que la protection effective des données est une condition essentielle au succès de ces politiques.

## Avant-propos



J'ai l'honneur de présenter au Parlement européen, au Conseil et à la Commission européenne le quatrième rapport annuel sur mes activités en qualité de Contrôleur européen de la protection des données, conformément au règlement (CE) n° 45/2001 du Parlement européen et du Conseil, et en application de l'article 286 du traité CE.

Le présent rapport couvre l'année 2007, qui est la troisième année complète d'activité depuis l'établissement du CEPD en tant que nouvelle autorité de contrôle indépendante, dont la mission est de veiller à ce que, lors du traitement des données à caractère personnel, les libertés et droits fondamentaux des personnes physiques, en particulier leur vie privée, soient respectés par les institutions et organes communautaires.

Le traité de Lisbonne, signé à la fin de l'année 2007, vise à assurer le caractère juridiquement contraignant de la charte des droits fondamentaux de l'Union européenne pour les institutions et organes, ainsi que pour les États membres lorsqu'ils mettent en œuvre le droit de l'UE. Ces deux instruments prévoient une protection renforcée des données à caractère personnel, et notamment des règles pour un contrôle indépendant.

Il s'agit là d'un repère important dans l'histoire de l'UE, qu'il convient également de considérer comme un défi. Les garanties fondamentales qui occupent une place privilégiée dans les traités doivent être mises en œuvre dans la pratique. Cela s'applique lorsque les institutions et organes concernés traitent des données à caractère personnel, mais aussi lorsqu'ils élaborent des règles et des politiques susceptibles d'avoir une incidence sur les droits et les libertés des citoyens européens.

Le présent rapport montre que — même en respectant les règles en vigueur en 2007 — les progrès accomplis en matière de supervision sont considérables. L'importance accordée à l'évaluation des résultats a encouragé la plupart des institutions et organes communautaires à prendre des mesures pour se conformer aux exigences en matière de protection des données. Si les mesures prises sont assez satisfaisantes, il convient néanmoins de poursuivre les efforts pour que ces exigences soient pleinement respectées.

En matière de consultation, l'accent a été mis en particulier sur la nécessité de mettre en place un cadre cohérent et efficace pour la protection des données, tant dans le premier que dans le troisième pilier, mais les résultats obtenus n'ont pas toujours été satisfaisants. Le rapport souligne aussi que les domaines d'action bénéficiant des activités consultatives du CEPD sont de plus en plus nombreux.

Je profite donc de l'occasion qui m'est donnée, cette année encore, pour remercier ceux qui, au sein du Parlement européen, du Conseil et de la Commission, soutiennent notre travail, ainsi que les nombreux membres des divers institutions et organes qui sont directement responsables de la manière dont la protection des données est mise en pratique. Je tiens également à encourager tous ceux qui sont chargés de relever les défis de demain.

Enfin, je tiens à remercier tout particulièrement, également au nom de M. Joaquín Bayo Delgado, le Contrôleur adjoint, les membres de notre personnel. Ceux-ci font preuve de qualités remarquables qui contribuent largement à notre efficacité.

Peter Hustinx  
*Contrôleur européen de la protection des données*

# 1. Bilan et perspectives

## 1.1. Aperçu général de 2007

Le cadre juridique dans lequel opère le Contrôleur européen de la protection des données (CEPD) <sup>(2)</sup> définit un certain nombre de tâches et de compétences qui permettent de distinguer trois fonctions principales. Ces fonctions conservent une valeur stratégique pour les activités du CEPD et sont présentées dans la rubrique liminaire sur l'énoncé de ses missions:

- une fonction de contrôle, qui consiste à exercer une supervision des institutions et organes communautaires <sup>(3)</sup> afin que ceux-ci respectent les garanties juridiques existantes chaque fois qu'ils traitent des données à caractère personnel;
- une fonction de consultation, qui consiste à conseiller les institutions et organes communautaires sur toutes les questions pertinentes, et en particulier sur les propositions législatives ayant une incidence sur la protection des données à caractère personnel;
- une fonction de coopération, qui consiste à travailler avec les autorités nationales de contrôle et les organes de contrôle relevant du troisième pilier de l'UE chargés de la coopération policière et judiciaire en matière pénale, en vue d'améliorer la cohérence en matière de protection des données à caractère personnel.

Ces fonctions sont exposées en détail dans les chapitres 2, 3 et 4 du présent rapport annuel, qui décrivent les principales activités du CEPD et les avancées réalisées en 2007. L'importance de l'information et de la communication en ce qui concerne ces activités nous a amenés à consacrer un chapitre entier à la communication (voir le chapitre 5). La plupart de ces activités reposent sur une gestion efficace des ressources financières, humaines et autres, qui font l'objet du chapitre 6.

<sup>(2)</sup> Voir l'aperçu du cadre juridique à l'annexe A et un extrait du règlement (CE) n° 45/2001 à l'annexe B.

<sup>(3)</sup> Les termes «institutions» et «organes» qui figurent dans le règlement (CE) n° 45/2001 sont utilisés tout au long du rapport. Ils désignent aussi les agences communautaires. Pour obtenir une liste complète de celles-ci, utilisez le lien: [http://europa.eu/agencies/community\\_agencies/index\\_fr.htm](http://europa.eu/agencies/community_agencies/index_fr.htm).

Le traité de Lisbonne, signé le 13 décembre 2007, a marqué la fin d'une réflexion sur le rôle, la structure et le fonctionnement de l'Union européenne. Le 12 décembre 2007, une version légèrement remaniée de la charte des droits fondamentaux de l'UE a été signée à Strasbourg. Bien que cette charte ne fasse plus partie du traité, elle est légalement contraignante pour l'ensemble des institutions et organes de l'UE, ainsi que pour les États membres lorsqu'ils mettent en œuvre la législation communautaire. La protection des données à caractère personnel, y compris la nécessité d'un contrôle indépendant, apparaît clairement dans les deux instruments et est censée avoir un impact horizontal. Le CEPD suivra de près, dans un futur proche, les progrès réalisés dans ce domaine.

La protection renforcée des données à caractère personnel, telle que prévue par le traité de Lisbonne, donne également l'occasion aux institutions de montrer comment elle est mise en pratique. Le CEPD a d'emblée souligné que la licéité du traitement des données à caractère personnel conditionne de nombreuses politiques de l'UE et qu'une protection effective des données à caractère personnel, en tant que valeur fondamentale qui sous-tend les politiques de l'UE, devrait être considérée comme une condition du succès de ces politiques. C'est cet esprit général qui continuera d'animer le CEPD, qui est heureux de constater un soutien de plus en plus important à cet égard.

En 2007, le contrôle préalable a encore constitué l'essentiel des activités de supervision. Le CEPD ayant fixé le printemps 2007 comme échéance pour l'examen de la conformité au règlement (CE) n° 45/2001, il a été constaté une augmentation impressionnante du nombre de notifications soumises en vue d'un contrôle préalable et, par conséquent, du nombre d'avis rendus par le CEPD. Le nombre de plaintes recevables a également considérablement augmenté. L'ensemble des institutions et organes communautaires, y compris certaines agences créées récemment, ont veillé à nommer un délégué à la protection des données (voir le chapitre 2).

Les activités consultatives ont, elles aussi, continué à se développer de manière satisfaisante. L'accent a été mis sur la nécessité de mettre en place un cadre cohérent et efficace pour la protection des données, tant dans le premier que

dans le troisième pilier. Cependant, pour ce dernier, les résultats n'ont pas été satisfaisants. À la suite de l'inventaire des propositions de la Commission, publié à la fin de 2006, le CEPD est intervenu dans un nombre croissant de domaines d'action, ce qui s'est traduit par un plus grand nombre d'avis, d'observations et autres activités à différentes phases du processus législatif. Par ailleurs, certaines affaires portées devant la Cour de justice des Communautés européennes ont requis une attention particulière (voir le chapitre 3).

La coopération avec les autorités nationales de contrôle s'est concentrée sur le rôle du groupe de l'article 29, ce qui a mené à l'adoption de textes importants sur des questions stratégiques. Le CEPD a joué un rôle majeur dans le contrôle coordonné d'Eurodac. Cette manière de procéder se révélera très utile pour d'autres systèmes d'information à grande échelle. Une attention particulière a également été accordée à une coopération renforcée dans le cadre de questions relevant du troisième pilier. Enfin, le CEPD a consacré beaucoup de temps au suivi de l'initiative de Londres, dont l'objectif est de mieux faire connaître la protection des données et de rendre celle-ci plus efficace (voir le chapitre 4).

## 1.2. Résultats obtenus en 2007

Le rapport annuel 2006 exposait les principaux objectifs figurant ci-après, qui avaient été retenus pour 2007. La plupart de ces objectifs ont été entièrement ou partiellement atteints.

### Champ d'activités du réseau des DPD

Le réseau des délégués à la protection des données (DPD) est devenu pleinement opérationnel, toutes les institutions et tous les organes communautaires, y compris les agences communautaires, participant à ses activités. Le CEPD a continué d'apporter un soutien sans faille et de prodiguer ses conseils afin de développer les fonctions exercées par les DPD, en accordant une attention toute particulière aux délégués récemment nommés.

### Poursuite des contrôles préalables

Si le nombre de contrôles préalables liés à des opérations de traitement existantes a nettement augmenté, la plupart des institutions et organes communautaires doivent encore poursuivre leurs efforts pour remplir leurs obligations dans ce domaine. Les résultats des contrôles préalables sont régulièrement communiqués aux DPD et aux autres parties concernées.

### Inspections et vérifications

Le CEPD a commencé à examiner les progrès réalisés dans la mise en œuvre du règlement (CE) n° 45/2001 à partir du printemps 2007. Cet exercice a porté sur l'ensemble des institutions et organes, l'accent étant mis notamment sur la phase de mise en œuvre propre à chacun d'entre eux. Les résultats ont été exposés de manière générale ainsi qu'au cas par cas (voir le chapitre 2).

### Vidéosurveillance

L'utilisation de la vidéosurveillance tant au niveau de l'UE qu'à celui des États membres a fait l'objet d'enquêtes, et différents cas impliquant des institutions ou organes ont été examinés. Ces travaux serviront de base aux projets d'orientations qui pourront être consultés sur le site internet du CEPD en 2008.

### Questions horizontales

Les avis relatifs aux contrôles préalables et les décisions concernant les plaintes sont systématiquement analysés pour identifier d'éventuelles questions horizontales. Les premiers documents formulant des conseils destinés à toutes les institutions et à tous les organes communautaires seront publiés en 2008. La question de la conservation de données médicales ou relatives à des mesures disciplinaires a été abordée avec les autorités compétentes.

### Consultation sur les propositions législatives

Le CEPD a continué de rendre des avis sur les propositions de nouvelles dispositions législatives et a assuré un suivi approprié. Ce rôle consultatif couvre un plus grand nombre de domaines et s'appuie sur un inventaire et une sélection systématiques des priorités, élaborés avec l'aide des services concernés de la Commission, et ce pour la seconde fois.

### Protection des données s'agissant du troisième pilier

Le CEPD a continué d'accorder une attention particulière à la mise en place et à l'adoption d'un cadre général pour la protection des données s'agissant du troisième pilier. Par ailleurs, il a régulièrement procédé à l'examen des propositions concernant l'échange de données à caractère personnel, notamment dans le contexte du traité de Prüm. Dans les deux cas, cela n'a malheureusement eu qu'une incidence limitée.

### Communiquer sur la protection des données

Le CEPD a apporté un soutien sans faille aux activités de suivi de l'initiative de Londres, dont l'objectif est de «communiquer sur la protection des données et la rendre plus efficace». Il s'agit d'actions visant à partager les «bonnes pratiques» en matière d'application et de développement stratégique avec les autorités chargées de la protection des données (DPA) de différents pays dans le monde.

### Règlement intérieur

L'élaboration d'un règlement intérieur tenant compte des différents rôles et activités du CEPD a pris plus de temps que prévu. La rédaction de divers manuels internes a cependant bien avancé. Le règlement intérieur sera adopté et publié en 2008, accompagné d'informations pratiques à l'intention des personnes intéressées qui seront publiées sur le site internet.

### Gestion des ressources

Le CEPD a continué d'améliorer la gestion des ressources financières et humaines en renforçant la structure budgétaire, en adoptant des règles internes concernant l'évaluation du

personnel et en mettant en place une politique de formation. La création d'un système de contrôle interne et la nomination d'un délégué à la protection des données sont autant d'autres progrès.

### 1.3. Objectifs en 2008

Les principaux objectifs figurant ci-après ont été retenus pour 2008. Les résultats obtenus seront analysés dans le prochain rapport annuel.

#### **Soutien au réseau des délégués à la protection des données**

Le CEPD continuera de soutenir pleinement les délégués à la protection des données, en particulier ceux des nouvelles agences, et les encouragera à poursuivre leurs échanges de compétences et de bonnes pratiques.

#### **Rôle du contrôle préalable**

Le CEPD a l'intention de terminer le contrôle préalable des opérations de traitement existantes pour la plupart des institutions et organes et de mettre l'accent sur la mise en œuvre de ses recommandations. Les résultats des contrôles préalables et du suivi seront partagés avec les DPD et les autres parties concernées.

#### **Directives horizontales**

Le CEPD élaborera des directives sur des questions pertinentes communes à la plupart des institutions et organes (par exemple, le traitement de données en matière de santé, l'octroi d'un accès aux personnes concernées et la question de la vidéosurveillance). Ces orientations seront largement diffusées et une série de séminaires sera organisée à l'intention des parties intéressées.

#### **Vérification du respect du règlement**

Le CEPD continuera de vérifier que le règlement (CE) n° 45/2001 est respecté, par le biais de différents types de contrôles selon les institutions et organes, et effectuera de plus en plus d'inspections sur le terrain. Le CEPD publiera également une politique générale d'inspection.

#### **Systèmes à grande échelle**

Le CEPD continuera de mettre en place un contrôle coordonné d'Eurodac, de concert avec les autorités de contrôle nationales, et d'acquérir les compétences nécessaires pour contrôler dans un proche avenir d'autres systèmes à grande échelle tels que le système d'information Schengen de deuxième génération (SIS II) et le système d'information sur les visas (VIS).

#### **Avis sur les propositions législatives**

Le CEPD continuera de rendre des avis ou de formuler des observations sur des propositions de nouvelles législations, sur la base d'un inventaire systématique des priorités et des sujets pertinents, et d'assurer un suivi approprié.

#### **Traité de Lisbonne**

Le CEPD continuera de suivre l'évolution du traité de Lisbonne, procédera à une analyse approfondie de son incidence sur la protection des données et fera, le cas échéant, des recommandations à ce sujet.

#### **Informations en ligne**

Le CEPD a l'intention d'actualiser les informations disponibles sur son site internet, d'en augmenter le nombre et de continuer d'améliorer le bulletin d'information électronique.

#### **Règlement intérieur**

Le CEPD adoptera et publiera un règlement intérieur s'appliquant à ses diverses fonctions et activités. Des outils pratiques destinés aux parties intéressées seront disponibles sur son site internet.

#### **Gestion des ressources**

Le CEPD consolidera et continuera de développer un certain nombre d'activités liées aux ressources financières et humaines, et il améliorera d'autres méthodes de travail internes. Des espaces de bureaux supplémentaires seront nécessaires pour accueillir le futur personnel.

## 2. Supervision

### 2.1. Introduction

La mission du Contrôleur européen de la protection des données consiste à contrôler, de manière indépendante, les opérations de traitement effectuées par les institutions ou organes communautaires, relevant en tout ou en partie du champ d'application du droit communautaire (à l'exclusion de la Cour de justice dans l'exercice de ses fonctions juridictionnelles). Le règlement (CE) n° 45/2001 (ci-après dénommé le «règlement») définit et confère un certain nombre de fonctions et de compétences qui permettent au CEPD de s'acquitter de sa tâche de contrôle.

Cette année encore, le contrôle préalable a constitué l'essentiel des activités de contrôle. Cette tâche comprend l'examen des activités exercées par les institutions et organes dans les domaines susceptibles de présenter des risques particuliers pour les personnes concernées, au sens de l'article 27 du règlement. Comme cela est expliqué ci-après, le contrôle des opérations de traitement déjà en place, ainsi que celles qui sont planifiées, donne une image exacte de la manière dont sont traitées les données à caractère personnel dans les institutions et organes. Le CEPD a effectué un contrôle préalable des opérations de traitement existantes dans la plupart des catégories pertinentes. Une attention particulière a été accordée aux systèmes interinstitutionnels et aux autres situations d'utilisation conjointe par les institutions et organes, en vue d'une rationalisation et d'une simplification des procédures. Les avis rendus par le CEPD permettent aux responsables du traitement d'adapter leurs opérations de traitement de manière à respecter le règlement. Le CEPD dispose également d'autres moyens, notamment le traitement des plaintes, la réalisation d'enquêtes ou d'inspections et les conseils concernant des mesures administratives.

Pour ce qui est des compétences qui lui sont conférées, le CEPD n'a ordonné aucune mesure et n'a émis aucun avertissement ni aucune interdiction, pas plus en 2007 qu'au cours des années précédentes, les responsables du traitement ayant mis en œuvre ses recommandations ou exprimé leur intention de le faire et prenant les mesures nécessaires à cette fin. La rapidité des réactions varie selon les cas. Le CEPD a mis en place un suivi systématique de ses recommandations.



M. Joaquín Bayo Delgado, Contrôleur adjoint.

### 2.2. Délégués à la protection des données

Le règlement prévoit que chaque institution et organe communautaire doit nommer au moins un délégué à la protection des données (article 24, paragraphe 1). À ce DPD, certaines institutions ont associé un assistant ou un adjoint. La Commission a également nommé un DPD pour l'Office européen de lutte antifraude (OLAF — direction générale de la Commission) et un «coordinateur de la protection des données» (CPD) dans chacune des autres directions générales (DG) pour coordonner tous les aspects de la protection des données au sein de la DG concernée.

Depuis plusieurs années, les délégués à la protection des données se rencontrent régulièrement afin d'échanger leurs



Les délégués à la protection des données lors de leur 20<sup>e</sup> réunion à Bruxelles (8 juin 2007).

expériences et d'examiner des questions horizontales. Ce réseau informel a continué de faire la preuve de son efficacité en termes de collaboration en 2007.

En 2007, le DPD de l'Office européen de police (Europol) a été accueilli dans le réseau, en qualité d'observateur.

Le CEPD a assisté à certaines réunions des DPD en 2007, à savoir: en mars [Agence européenne pour la sécurité maritime (EMSA), à Lisbonne], en juin (Conseil, à Bruxelles) et en octobre [Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles) (OHMI), à Alicante]. Il a saisi cette occasion pour informer les DPD au sujet de son travail et pour examiner des questions d'intérêt commun. Il a profité de ces réunions pour expliquer la procédure de contrôle préalable et analyser certaines des principales questions soulevées dans le cadre de ce type de contrôle. En particulier, le champ d'application de l'article 27 a été précisé, notamment avec des exemples tels que les systèmes de communication électronique, les systèmes d'audit interne et les enquêtes effectuées par les DPD. Ces réunions ont aussi donné au CEPD l'occasion de souligner les progrès réalisés en matière de traitement des dossiers devant faire l'objet d'un contrôle préalable et de fournir des informations détaillées sur certaines conclusions tirées de l'activité de contrôle préalable (voir le point 2.3).

Le CEPD a également communiqué aux DPD des informations concernant les opérations d'inspection dans le cadre de l'échéance fixée au printemps 2007 (voir le point 2.6.1). Il a expliqué l'objectif poursuivi par ces inspections, décrit la méthodologie à adopter et évoqué les actions ciblées qui pourraient suivre. Au cours des réunions des DPD, ceux-ci ont également pu donner des informations sur l'incidence de ces inspections au sein de leur propre institution ou

agence, ce qui a permis au CEPD de prendre en compte certains éléments.

Un quatuor de délégués à la protection des données, composé de quatre DPD (Parlement européen, Conseil, Commission européenne et OHMI) a été désigné afin de coordonner le réseau des DPD. Le CEPD a étroitement collaboré avec ce quatuor, notamment pour établir l'ordre du jour des réunions.

Immédiatement après la réunion qui a eu lieu au mois de juin à Bruxelles, le CEPD a organisé, avec le concours de quelques DPD expérimentés, un atelier à l'intention des nouveaux délégués à la protection des données. Les principaux aspects du règlement ont été examinés, en mettant l'accent sur les questions pratiques susceptibles d'aider les nouveaux DPD dans la définition de leurs tâches. Les principales missions d'un DPD ont également été expliquées, et les formulaires de notification, les registres des notifications au DPD et les outils TI (technologie de l'information) ont été présentés.

Le groupe de travail sur les délais de conservation des données, leur verrouillage et leur effacement a organisé six ateliers en 2007, auxquels ont pris part le Contrôleur adjoint et deux membres du personnel. Un projet de document sur les conclusions des travaux du sous-groupe a été rédigé et sera communiqué en 2008 par les membres du groupe de travail aux personnes désignées au sein de leur institution ou organe (spécialistes IT, par exemple). Un document concernant les règles pertinentes en matière de délais et de verrouillage a également été préparé et examiné par les membres du groupe.

Dans le cadre de l'opération d'inspection «printemps 2007», le CEPD a souligné que chaque institution ou organe de l'UE était légalement tenu de nommer un DPD (voir le point 2.6.1).

## 2.3. Contrôles préalables

### 2.3.1. Base juridique

#### Principe général: article 27, paragraphe 1

L'article 27, paragraphe 1, du règlement dispose que tous «les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités» doivent être soumis au contrôle préalable du CEPD. L'article 27, paragraphe 2, énumère les traitements susceptibles de présenter de tels risques.

Cette liste n'est pas exhaustive. En effet, d'autres cas, qui ne sont pas mentionnés, pourraient présenter des risques particuliers au regard des droits et libertés des personnes concernées et, par conséquent, justifier un contrôle préalable du CEPD. Par exemple, tout traitement de données à caractère personnel qui touche au principe de confidentialité visé à l'article 36 implique des risques particuliers qui justifient un contrôle préalable du CEPD.

Un autre critère, qui a été adopté en 2006, est la présence de certaines données biométriques autres que les seules photographies, étant donné que la nature de la biométrie, les possibilités d'établir des interconnexions et la situation actuelle en termes d'outils technologiques peuvent avoir des conséquences inattendues ou non souhaitables pour les personnes concernées.

#### Cas énumérés à l'article 27, paragraphe 2

L'article 27, paragraphe 2, énumère un certain nombre de traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, à savoir:

- a) les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté <sup>(4)</sup>;
- b) les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement;
- c) les traitements permettant des interconnexions non prévues en vertu de la législation nationale ou commu-

nautaire entre des données traitées pour des finalités différentes;

- d) les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat.

Les critères élaborés au cours des années précédentes ont continué d'être appliqués pour l'interprétation de cette disposition, tant pour décider qu'un cas notifié par un DPD ne devait pas faire l'objet d'un contrôle préalable que pour émettre un avis dans le cadre d'une consultation sur la nécessité de procéder à un tel contrôle (voir le point 2.3.6).

### 2.3.2. Procédure

#### Notification/consultation

Les contrôles préalables doivent être effectués par le CEPD après réception de la notification du délégué à la protection des données.

#### Délai, suspension et prolongation

Le CEPD doit rendre son avis dans les deux mois qui suivent la réception d'une notification. Lorsqu'il demande des informations complémentaires, le délai de deux mois est généralement suspendu jusqu'à ce que les informations en question aient été communiquées. Cette période de suspension comprend le délai [qui est généralement de sept à dix jours <sup>(5)</sup> accordé au DPD de l'institution ou de l'organe concerné pour formuler ses observations — et fournir le cas échéant des informations complémentaires — sur le projet final].

Lorsque la complexité du dossier l'exige, le délai de deux mois peut lui aussi être prolongé pour une nouvelle période de deux mois sur décision du CEPD, qui doit être notifiée au responsable du traitement avant l'expiration du délai initial de deux mois. Si, au terme de deux mois, éventuellement prolongé, aucune décision n'a été rendue, l'avis du CEPD est réputé favorable. Jusqu'à présent, ce cas de figure où l'avis serait rendu de manière tacite ne s'est jamais produit.

Pour les cas examinés a posteriori reçus avant le 1<sup>er</sup> septembre 2007, le mois d'août a été exclu des calculs, tant pour les institutions et organes que pour le CEPD, en raison de l'énorme quantité de dossiers soumis (voir le point 2.3.3).

#### Registre

L'article 27, paragraphe 5, du règlement prévoit que le CEPD doit tenir un registre de tous les traitements qui lui sont notifiés en vue d'un contrôle préalable. Ce registre doit contenir les informations visées à l'article 25 et pouvoir être accessible au public pour consultation.

<sup>(4)</sup> *Security* en anglais, à savoir des mesures adoptées dans le cadre d'une procédure judiciaire.

<sup>(5)</sup> Jours ouvrables, lorsqu'ils coïncident avec des périodes de vacances.

Ce registre a pour base un formulaire de notification qui doit être rempli par les DPD et transmis au CEPD. Le besoin d'informations complémentaires est ainsi réduit le plus possible.

Par souci de transparence, toutes les informations sont consignées dans le registre (à l'exception des mesures de sûreté) et sont accessibles au public.

Une fois que le CEPD a exprimé son avis, celui-ci est rendu public. Par la suite, les modifications apportées par le responsable du traitement à la lumière de l'avis du CEPD sont aussi indiquées sous une forme synthétique. Deux objectifs sont ainsi réalisés: d'une part, les informations relatives à un traitement donné sont tenues à jour; d'autre part, le principe de transparence est respecté.

Toutes ces informations seront publiées sur le nouveau site internet du CEPD, ainsi qu'un résumé du dossier concerné.

## Avis

Conformément à l'article 27, paragraphe 4, du règlement, la position finale du CEPD revêt la forme d'un avis qui doit être notifié au responsable du traitement et au délégué à la protection des données de l'institution ou de l'organe concerné.

Les avis sont structurés de la façon suivante: une description de la procédure; un résumé des faits; une analyse juridique; des conclusions.

L'analyse juridique consiste, d'abord, à déterminer si le cas remplit bien les conditions requises pour pouvoir faire l'objet d'un contrôle préalable. Comme cela est précisé plus haut, si le cas en question ne relève pas des cas énumérés à l'article 27, paragraphe 2, le CEPD examinera les risques qui en découlent pour les droits et libertés de la personne concernée. Lorsque le cas remplit les conditions requises pour pouvoir faire l'objet d'un contrôle préalable, l'analyse juridique consiste principalement à déterminer si le traitement est conforme aux dispositions pertinentes du règlement. Si nécessaire, des recommandations sont formulées en vue de garantir le respect du règlement. Dans ses conclusions, le CEPD a jusqu'à présent, en règle générale, déclaré que le traitement en question ne paraissait pas entraîner de violation d'une disposition quelconque du règlement, pour autant qu'il soit tenu compte des recommandations émises. Les conclusions n'ont été différentes que pour deux avis rendus en 2007 (dossiers de contrôle préalable proprement dit n° 2007-373 et 2007-680, voir ci-après): les traitements concernés violaient le règlement, et leur mise en conformité avec celui-ci nécessitait la mise en œuvre de certaines recommandations.

Pour la première fois, en 2007, des modifications apportées dans des traitements ayant fait l'objet d'un contrôle préalable ont été notifiées. Pour les avis concernant ces dossiers, une forme synthétisée a été mise au point.

Un manuel a été élaboré afin de garantir, comme dans d'autres domaines, que l'ensemble du personnel travaille dans des conditions identiques et que les avis du CEPD sont adoptés à l'issue d'une analyse complète de toutes les informations pertinentes. Ce manuel présente la structure des avis, en se fondant sur une somme d'expériences pratiques, et fait l'objet d'une mise à jour permanente. Il comporte aussi une liste de contrôle.

Un système de gestion des tâches a été mis en place pour s'assurer que toutes les recommandations relatives à un dossier donné sont mises en œuvre et, le cas échéant, que toutes les décisions sont respectées (voir le point 2.3.7).

Distinction entre les cas examinés a posteriori et les cas de contrôle préalable proprement dit, et définition de catégories différentes.

Le règlement est entré en vigueur le 1<sup>er</sup> février 2001. Conformément à l'article 50, les institutions et organes communautaires devaient prendre les mesures nécessaires pour que les opérations de traitement déjà en cours à cette date soient mises en conformité avec le règlement dans un délai d'un an à compter de ladite date (soit le 1<sup>er</sup> février 2002). Or, la nomination du CEPD et du Contrôleur adjoint a pris effet le 17 janvier 2004.

Les contrôles préalables concernent non seulement les traitements qui ne sont pas encore en cours (contrôles préalables proprement dits), mais aussi ceux qui ont débuté avant le 17 janvier 2004 ou avant l'entrée en vigueur du règlement (cas examinés a posteriori). Dans de tels cas, un contrôle au titre de l'article 27 ne pourrait être «préalable» au sens strict du terme, il doit donc être réalisé a posteriori. Adopter cette approche pragmatique permet au CEPD de garantir le respect de l'article 50 du règlement pour ce qui est des traitements présentant des risques particuliers.

Afin de résorber l'arriéré des cas susceptibles de faire l'objet d'un contrôle préalable, le CEPD a demandé aux DPD d'analyser la situation dans leurs institutions respectives en ce qui concerne les opérations de traitement relevant du champ d'application de l'article 27 depuis 2004. Après réception des contributions de tous les DPD, une liste des dossiers devant faire l'objet d'un contrôle préalable a été établie et précisée par la suite.

À l'issue de l'inventaire, certaines catégories ont été recensées dans la plupart des institutions et organes; on a donc estimé qu'elles se prêtaient à un contrôle plus systématique:

- 1) dossiers médicaux (tant les dossiers médicaux au sens strict que les dossiers contenant des données relatives à la santé);
- 2) évaluation du personnel (dont le futur personnel — recrutement);
- 3) infractions et suspicions, y compris les procédures disciplinaires;
- 4) services sociaux;
- 5) contrôle des communications électroniques.



L'équipe de contrôle en réunion.

Ces catégories ont été considérées en 2005 et en 2006 comme des catégories prioritaires, mais pour donner plein effet à l'échéance fixée au printemps 2007, elles ne s'appliquent plus à la définition de priorités et sont plutôt utilisées pour les contrôles systématiques. Ces catégories n'ont jamais été appliquées aux cas de contrôle préalable proprement dit, ceux-ci devant être examinés avant que l'opération de traitement concernée ne soit mise en œuvre.

### 2.3.3. Évaluation quantitative

#### Notifications de contrôle préalable

Comme indiqué dans les rapports annuels 2005 et 2006, le CEPD a constamment encouragé les DPD à lui adresser davantage de notifications en vue d'un contrôle préalable.

L'échéance pour la réception des notifications en vue d'un contrôle préalable du CEPD — cas examinés a posteriori — a été fixée au printemps 2007 afin d'encourager les institutions et les organes communautaires à redoubler d'efforts en vue de respecter pleinement leur obligation de notification.

Il en a résulté une augmentation significative du nombre de notifications: 132 entre le 1<sup>er</sup> janvier et le 30 juin 2007, contre un total de 137 soumises jusqu'alors (dont 32 durant le second semestre de 2006), auxquelles 44 autres se sont ajoutées au cours du second semestre de 2007. L'échéance fixée au printemps 2007 a donc eu pour effet que 208 notifications (132 + 32 + 44) sur 313 ont été soumises entre 2004 et la fin de 2007.

#### Avis rendus en 2007 sur des cas de contrôle préalable

En 2007, **90 avis** <sup>(6)</sup> ont été rendus sur des notifications adressées en vue d'un contrôle préalable.

Ces 101 cas qui ont abouti à un avis officiel représentent par rapport à 2006 une augmentation de 77,19 % des dossiers de contrôle préalable. Cette augmentation de la charge de travail est certainement liée à l'échéance fixée au printemps 2007 <sup>(7)</sup>.

Sur les 101 cas de contrôle préalable (90 avis), onze étaient des cas de contrôle préalable proprement dit, c'est-à-dire que les institutions concernées (Cour des comptes, Parlement, EPSO, Médiateur européen, ETF, BCE, BEI et OLAF, et trois pour la Commission) ont suivi la procédure relative au contrôle préalable avant la mise en œuvre de l'opération de traitement:

— parmi ces onze cas de contrôle préalable, quatre (à savoir les trois de la Commission et celui de l'ETF) concernaient le système de flexitime;

— deux autres avaient pour objet l'insuffisance professionnelle;

— les autres portaient sur la nécessité de faire état de la connaissance d'une troisième langue pour être promu, la gestion des congés, les règles en matière d'habilitation de sécurité, les dossiers médicaux et la gestion des services, et le système de notification des fraudes (voir le point 2.3.5).

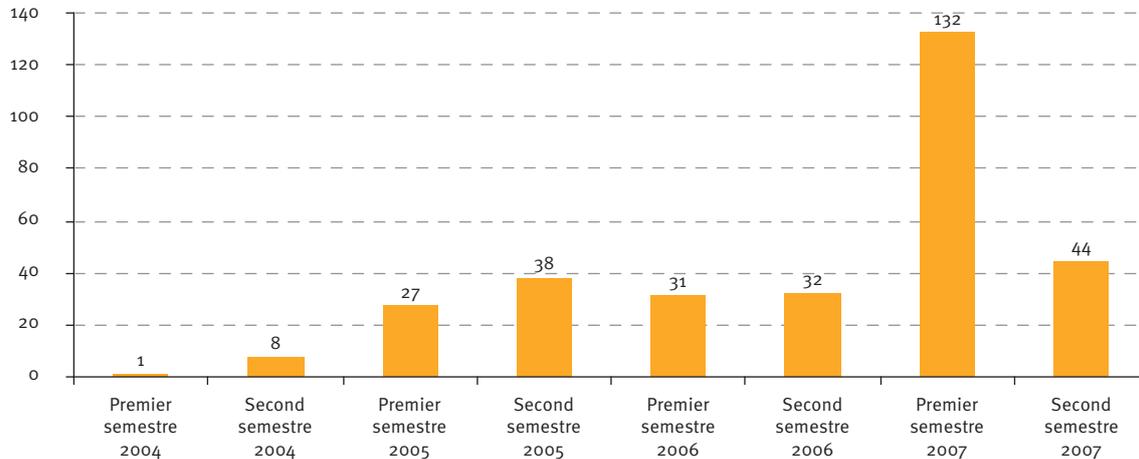
Il convient de noter que les deux opérations de traitement qui ne respectaient pas le règlement se trouvent parmi ces onze cas de contrôle préalable proprement dit (l'un relatif à un flexitime en particulier, l'autre aux dossiers médicaux). Les 90 autres dossiers (79 avis) ont fait l'objet d'un contrôle préalable a posteriori.

Outre ces 101 dossiers de contrôle préalable sur lesquels un avis a été rendu, le CEPD en a traité 31 qui ont été considérés comme ne devant pas faire l'objet d'un contrôle préalable, ce qui représente un pourcentage assez élevé (23,48 % des 132 dossiers soumis au CEPD en 2007), parmi lesquels 11 concernent des dossiers relatifs au contrôle des communications électroniques. L'analyse de ces 31 dossiers est détaillée au point 2.3.7.

<sup>(6)</sup> Sur 101 notifications, pour des raisons pratiques et vu le lien existant entre certains cas, 15 notifications adressées par l'OLAF ont été traitées conjointement dans quatre avis différents. C'est pourquoi 90 avis ont été rendus pour 101 notifications.

<sup>(7)</sup> Voir le point 2.3.7 pour les 31 autres cas examinés en 2007.

## Notifications adressées au CEPD



Conseil de l'Union européenne	3 dossiers
Commission européenne	19 dossiers
Banque centrale européenne (BCE)	5 dossiers
Cour de justice des Communautés européennes (CJCE)	5 dossiers
Banque européenne d'investissement (BEI)	1 dossier
Parlement européen	11 dossiers
Centre de traduction des organes de l'Union européenne (CdT)	1 dossier
Office de sélection du personnel des Communautés européennes (EPSO) (*)	1 dossier
Cour des comptes européenne	3 dossiers
Comité des régions (CdR)	4 dossiers
Médiateur européen	7 dossiers
Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles) (OHMI)	7 dossiers
Office européen de lutte antifraude (OLAF)	25 dossiers (14 avis)
Office communautaire des variétés végétales (OCVV)	1 dossier
Autorité européenne de sécurité des aliments (EFSA)	1 dossier
Observatoire européen des drogues et des toxicomanies (OEDT)	1 dossier
Agence européenne des médicaments (EMA)	2 dossiers
Agence européenne pour la sécurité maritime (EMSA)	2 dossiers
Fondation européenne pour la formation (ETF)	2 dossiers

(\*) EPSO fait appel au délégué de la Commission.

### Analyse par institution et organe

La plupart des institutions et organes ont notifié des opérations de traitement susceptibles de présenter des risques spécifiques. Le travail considérable effectué en 2007 pour rendre des avis concernant des contrôles préalables est la

suite logique du grand nombre de notifications soumises par les DPD. La Commission européenne a fait des progrès remarquables dans ce domaine, bien qu'un nombre important de notifications soient toujours attendues. Le Parlement européen, l'OLAF et le Médiateur européen ont également soumis un grand nombre de notifications. Parmi les agences européennes, l'OHMI s'est montré très actif en matière de notification d'opérations de traitement. D'autres agences ont commencé à notifier des opérations de traitement. Les avis correspondants seront rendus en 2008 (voir ci-après «Notifications adressées en vue d'un contrôle préalable reçues avant le 1<sup>er</sup> janvier 2008 et en cours d'examen» et le point 2.6).

### Analyse par catégorie

Les dossiers de contrôle préalable traités se répartissent comme suit, par catégorie:

Première catégorie (dossiers médicaux)	16 dossiers
Deuxième catégorie (évaluation du personnel)	41 dossiers
Troisième catégorie (infractions et suspicions)	14 dossiers
Quatrième catégorie (services sociaux)	8 dossiers
Cinquième catégorie (contrôle des communications électroniques)	4 dossiers
Autres domaines	7 dossiers

La **première catégorie** comprend le dossier médical à proprement parler et son contenu (cinq dossiers), les absences pour maladie (trois dossiers), la procédure d'invalidité (un dossier), les crèches (un dossier), les régimes d'assurance maladie (un dossier), la dosimétrie des rayonnements (un dossier) et quatre dossiers concernant des données relatives à la santé. Le pourcentage que représente cette catégorie par rapport à l'ensemble décroît d'année en année (passant de 26,5 % des dossiers soumis en 2005 à 24,6 % en 2006 et à

17,77 % en 2007), mais elle a permis au CEPD de donner des conseils sur le contenu des dossiers médicaux. En 2007, le CEPD s'est penché sur un dossier lié à la dosimétrie des rayonnements au Centre commun de recherche, qui ne manquera pas d'être suivi par d'autres.

La catégorie la plus représentée reste la **deuxième**, relative à l'évaluation du personnel (41 dossiers sur les 90), affichant un pourcentage relativement stable (56 % des dossiers en 2005, contre 40,4 % en 2006 et 45,55 % en 2007). Dix dossiers concernaient le recrutement (de stagiaires, d'experts nationaux détachés, de personnel d'encadrement supérieur, ainsi que le recrutement à la BCE et à l'OCVV), cinq dossiers étaient relatifs à l'évaluation, trois aux promotions, deux à l'insuffisance professionnelle (tous deux des cas de contrôle préalable proprement dit), huit aux procédures de certification et d'attestation, quatre au flexitime (tous des cas de contrôle préalable proprement dit), deux à la retraite anticipée et, enfin, sept portaient sur d'autres questions.

Pour ce qui est de la **troisième catégorie** (concernant les infractions et les suspicions), on a pu constater une augmentation sensible du nombre de dossiers (quatorze avis, ce qui représente 15,55 % du total), mais il convient de souligner que cette catégorie comprend presque tous les dossiers soumis par l'OLAF (voir le point 2.3.4). Seuls deux avis ont été rendus sur des procédures disciplinaires, la plupart des institutions ayant déjà notifié ce type de dossiers au cours des années précédentes.

Concernant la **quatrième catégorie** (services sociaux), le nombre de notifications a été multiplié par quatre (huit avis, ce qui représente 8,88 % du nombre total d'avis). Toutes les institutions principales, y compris l'OHMI, ont respecté l'obligation de notification dans ce domaine. Il apparaît que la plupart des agences ne sont pas en mesure d'offrir ce type de services à leur personnel.

Pour ce qui est de la **cinquième catégorie** (contrôle des communications électroniques), seuls quatre avis ont été rendus, le CEPD ayant estimé que la plupart de ces notifications ne devaient pas être soumises à un contrôle préalable au motif que les opérations de traitement visées ne présentaient pas de risques particuliers — violation de la confidentialité en vertu de l'article 27, paragraphe 1, du règlement ou suspicion d'infraction en vertu de l'article 27, paragraphe 2, point a), du règlement ou évaluation de caractéristiques personnelles conformément à l'article 27, paragraphe 2, point b). Toutefois, l'analyse du CEPD a débouché sur de nombreuses recommandations (voir le point 2.3.7).

En ce qui concerne les notifications ne relevant pas de ces catégories, le CEPD a continué d'analyser des dossiers ayant trait à des questions financières, notamment l'instance spécialisée en matière d'irrégularités financières (Parlement et CJCE), le système d'alerte rapide (SAR) (Parlement et OLAF) et la procédure de passation des marchés (Conseil). Les autres dossiers abordés concernaient la participation à une grève (Conseil) et les règles en matière d'habilitation de sécurité (BCE).

## Délais du CEPD et des institutions

Les trois graphiques de l'annexe E illustrent les délais pour les travaux du CEPD et des institutions et organes communautaires. Ils fournissent des informations détaillées sur le nombre de jours de travail du CEPD nécessaires à l'élaboration des avis, le nombre de jours de prolongation requis par le CEPD et le nombre de jours de suspension (temps nécessaire à la réception des informations adressées par les institutions et organes).

*Nombre de jours de travail pour l'élaboration d'un avis du CEPD:* ce nombre est en diminution de 1,73 %, soit un jour de moins qu'en 2006 (55,5 jours de travail en 2005, 57,9 en 2006 et 56,9 en 2007), ce qui est très satisfaisant, compte tenu de l'augmentation du nombre des notifications transmises au CEPD et de leur complexité croissante.

*Nombre de jours de travail dans le cadre d'une prolongation du délai prévu pour l'avis du CEPD:* ce nombre est en diminution de 15,74 %, presque un jour de moins qu'en 2006 (3,3 jours en 2005, 5,4 en 2006 et 4,55 en 2007). Par ailleurs, bien que la période de prolongation puisse être de deux mois au maximum (article 27, paragraphe 4, du règlement), elle a généralement duré moins d'un mois.

*Nombre de jours écoulés dans le cas d'une suspension du délai prévu:* depuis la mi-2006, ce nombre comprend le délai de 7 ou 10 jours accordé au DPD pour faire part de ses observations sur le projet final et communiquer des informations complémentaires. Pour les cas examinés a posteriori reçus avant le 1<sup>er</sup> septembre 2007, le mois d'août n'est pas compris dans le calcul. L'augmentation constatée entre 2006 (72,8 jours en moyenne par dossier) et 2007 (75,14 jours en moyenne) est de 3,21 %. Compte tenu de ce que, en 2005, la moyenne était de 29,8 jours de travail par dossier, le CEPD est préoccupé par le temps que mettent les institutions et organes à transmettre les informations complémentaires demandées, en particulier dans trois cas (respectivement 185, 200 et 203 jours). En tout état de cause, il rappelle une fois encore aux institutions et organes qu'ils sont obligés de coopérer avec lui et de lui communiquer les informations demandées, conformément à l'article 30 du règlement.

*Moyenne par institution:* pour 2007, les tableaux montrent que, pour certaines institutions et certains organes, le nombre de jours de suspension a considérablement augmenté (Parlement, CdR, Cour des comptes, CdT et quelques autres dans une moindre mesure, notamment BCE et Commission), tandis que, pour d'autres, il a diminué (OHMI, BEI, CJCE et Conseil).

## Notifications adressées en vue d'un contrôle préalable reçues avant le 1<sup>er</sup> janvier 2008 et en cours d'examen

À la fin de l'année 2007, **69 cas de contrôle préalable** étaient déjà en cours de traitement. Parmi ceux-ci, 4 notifications

avaient été adressées en 2006 et 65 en 2007. Parmi ces 69 dossiers en cours d'examen, 25 avaient déjà abouti à un avis avant la fin février 2008.

OLAF	4 dossiers
Parlement	4 dossiers
Conseil	9 dossiers
Commission	23 dossiers
BCE	1 dossier
CESE et CdR	3 dossiers
BEI	3 dossiers
Cour des comptes	2 dossiers
CJCE	2 dossiers
Médiateur européen	1 dossier
Cedefop	1 dossier
OCVV	2 dossiers
EFSA	1 dossier
OEDT	1 dossier
EMEA	7 dossiers
EMSA	2 dossiers
EPSO	1 dossier
OHMI	1 dossier
CdT	1 dossier

### Analyse par institution et organe

Comme indiqué plus haut, l'échéance fixée au printemps 2007 a eu pour effet qu'un nombre croissant d'agences ont entamé le processus de notification (Cedefop, OEDT, EMEA — en particulier, avec 7 notifications — et EMSA) ou continué de le mettre en œuvre (CdT, EFSA et OCVV). Le CEPD encourage les autres agences et organes à faire de même.

Le nombre de dossiers notifiés par le Conseil et la Commission est important. En ce qui concerne la Commission, 16 des 27 dossiers émanent des différents sites des centres communs de recherche (CCR) et ont principalement trait à deux questions — dosimétrie des rayonnements et contrôle de l'accès — liées au contexte particulier des CCR (une des directions de la DG Recherche disposant d'une large autonomie).

### Analyse par catégorie

Les cas de contrôle préalable notifiés en cours au 1<sup>er</sup> janvier 2008 se répartissent comme suit, par catégorie prioritaire:

Première catégorie (dossiers médicaux)	20 dossiers
Deuxième catégorie (évaluation du personnel)	25 dossiers
Troisième catégorie (infractions et suspicions)	4 dossiers

Quatrième catégorie (services sociaux)	Néant
Cinquième catégorie (contrôle des communications électroniques)	3 dossiers
Autres domaines	17 dossiers

Dans la **première catégorie**, la persistance du processus de notification suscite les observations suivantes:

- cette catégorie représente 28,98 % des dossiers en cours au début de l'année 2008;
- un dossier, concernant le dossier médical de la Commission, présente une dimension interinstitutionnelle pour certains aspects spécifiques (par exemple archivage des dossiers médicaux);
- parmi ces vingt dossiers faisant l'objet d'un contrôle préalable, huit émanent de différents sites de CCR et concernent des domaines divers, tels que le dossier médical personnel (pour l'ensemble des CCR), les premiers secours et les accidents, l'absence pour maladie et la procédure d'invalidité, et trois autres ont trait à la dosimétrie des rayonnements;
- le CEPD se félicite que des notifications relatives à ces domaines lui soient également adressées par des agences telles que l'OCVV et l'EMEA;
- par contre, il attend toujours la notification de la part de l'Office de gestion et de liquidation des droits individuels (PMO) mentionné dans le dernier rapport annuel.

La **deuxième catégorie** représente toujours la majorité des dossiers — exactement un tiers. Huit de ces dossiers portent sur les procédures de recrutement (utilisation des listes de réserve d'EPSO par les institutions) et sur les procédures de recrutement par les agences. Toutes les procédures d'évaluation en cours concernent des agences (OEDT, OCVV, EMEA, EMSA et EFSA). Deux autres notifications ont trait au flexitime (voir le point 2.3.5). En 2008, le CEPD aura pour la première fois l'occasion d'examiner une notification relative à la politique en matière de formation (dossier 2007-584 du Conseil).

En ce qui concerne la **troisième catégorie**, le CEPD se penche sur des dossiers de l'OLAF ainsi que sur la procédure disciplinaire et les enquêtes administratives du Cedefop. Il encourage les autres agences et organes à notifier leurs dossiers.

Quant à la **quatrième catégorie**, le CEPD n'est pas surpris de n'avoir aucune notification en cours, les agences lui ayant expliqué dans le cadre de l'échéance fixée au printemps 2007 et au-delà (voir le point 2.6) qu'elles n'étaient bien souvent pas en mesure d'offrir ce type de services à leur personnel.

La **cinquième catégorie** revêt toujours une importance particulière. En 2007, le CEPD a organisé de nombreuses réunions concernant le contrôle des communications électro-

niques et mis en place un exercice interactif visant à sensibiliser davantage le personnel à ce sujet. Une synthèse des conclusions de cet exercice sera publiée en 2008.

La catégorie «**Autres domaines**» (24,63 % des dossiers) comprend trois domaines principaux: les appels d'offres, la vidéosurveillance et les systèmes de contrôle de l'accès. Ces deux derniers domaines sont particulièrement importants: un document relatif à la vidéosurveillance sera publié en 2008 (voir le point 2.9), et le contrôle de l'accès est un sujet particulièrement sensible, ce contrôle faisant parfois appel à l'identification par radiofréquence (RFID) ou à la biométrie. En outre, le CEPD pourra, pour la première fois, publier un avis sur le traitement des données concernant des «personnes politiquement exposées» au sein de la BEI, une question également très sensible.

### 2.3.4. Principales questions soulevées par les cas examinés a posteriori

Les **données médicales et autres données relatives à la santé** sont traitées par les institutions et organes. Toute donnée liée directement ou indirectement à l'état de santé d'une personne relève de cette catégorie. Ainsi, les absences pour maladie et les demandes de remboursement des frais médicaux sont également soumises au contrôle préalable. Dans cette catégorie, le CEPD a en outre examiné des dossiers relatifs à la procédure d'invalidité, à la dosimétrie des rayonnements et aux crèches.

Tous ces contrôles préalables ont permis au CEPD d'analyser de manière approfondie des questions relatives au traitement de données médicales par les institutions et organes communautaires. Il s'est interrogé quant à la pertinence de certaines questions posées lors des visites médicales d'engagement et des visites médicales annuelles au vu des objectifs de ces visites. Il a ainsi examiné le rôle préventif de l'examen médical d'engagement et a recommandé qu'en principe cet examen ne soit pas effectué à des fins de prévention sans le consentement de la personne concernée. Le CEPD a également demandé que les questions concernant les membres de la famille qui n'ont pas de lien génétique avec la personne concernée n'apparaissent plus dans les questionnaires médicaux.

Pour ce qui est de la visite médicale annuelle, le CEPD estime qu'il convient de la considérer comme un service préventif, uniquement fondé sur le consentement de la personne concernée. Les visites médicales annuelles ne devraient pas, en règle générale, avoir pour objectif de certifier l'aptitude au travail, même si dans certains cas exceptionnels et bien précis — par exemple, si l'employé est exposé à des substances dangereuses — des tests et une certification spécifiques sont permis.

Les périodes de conservation des données médicales ont également fait l'objet de recommandations dans les avis de contrôle préalable rendus par le CEPD sur la base de celui

qu'il a rendu au collège des chefs d'administration (dossier 2006-532) <sup>(8)</sup>. En particulier, les données médicales collectées lors de la visite médicale d'embauche de candidats n'ayant pas été recrutés ne devraient être conservées que pendant une période limitée.

La question de la qualité des données contenues dans le dossier médical a également été posée dans le cadre de différents dossiers de contrôle préalable. Le CEPD a conclu que, bien qu'il soit difficile de parler d'exactitude des données médicales, le principe de qualité des données suppose notamment que la personne concernée a le droit de demander que l'avis d'un autre médecin et toute autre information pertinente soient ajoutés au dossier, afin de veiller à ce que les données soient à jour.

Une question précise portant sur le transfert de données à caractère personnel a été soulevée dans l'avis relatif au remboursement des frais médicaux (dossier 2004-238 de la Commission). Dans le cadre d'une procédure de plainte, prévue par l'article 90, paragraphe 2, du statut des fonctionnaires des Communautés européennes, le CEPD a recommandé que les informations permettant d'identifier la personne concernée soient supprimées lors de la transmission des données au comité de direction, ces données ne lui étant pas nécessaires pour rendre son avis.

Le **recrutement du personnel** est, pour des raisons évidentes, une opération de traitement commune à toutes les institutions et à tous les organes. La procédure de recrutement interinstitutionnelle d'EPSO a fait l'objet d'un examen et d'un avis du CEPD (dossier 2004-0236). En 2007, le Parlement et la BCE ont notifié, en vue d'un contrôle préalable, le traitement des données à caractère personnel dans le cadre de l'utilisation des listes de réserve d'EPSO. L'OLAF a également notifié sa procédure de recrutement d'agents temporaires à partir de listes de réserve spécifiques. La proportionnalité de la politique de l'OLAF en matière d'habilitation de sécurité pour le personnel a été remise en question notamment dans le cas des membres du personnel qui n'ont pas besoin d'avoir accès à des informations hautement confidentielles sur la base de la législation communautaire applicable.

Le CEPD a également effectué un contrôle préalable de la procédure de recrutement du personnel d'encadrement supérieur en vigueur à la Commission (dossier 2007-0193). Dans son avis, il rappelle que les candidats devraient pouvoir accéder à l'intégralité de leur dossier, y compris aux grilles et aux notes d'évaluation que les divers comités compétents ont dressées à leur sujet. Le CEPD est conscient que cette règle connaît une limitation, à savoir le principe de la confidentialité des travaux du jury, consacré par l'article 6 de l'annexe III du statut. Conformément à l'article 20, paragraphe 1, point c), du règlement, aucune note attribuée individuellement par les membres du jury ne devrait être

<sup>(8)</sup> Voir le rapport annuel du CEPD pour 2006, p. 35. Voir également la liste de conservation commune au point 2.7.

communiquée, pas plus que des informations comparant la personne concernée avec d'autres candidats.

**Évaluation du personnel:** à l'occasion de l'examen du dossier concernant «Sysper 2 promotions» de la Commission, le CEPD a formulé des recommandations relatives à la rétention de données et demandé à la Commission d'analyser la nécessité d'indiquer les procédures disciplinaires en cours dans le système comme motif de suspension de l'exercice de promotion <sup>(9)</sup>.

Le CEPD a continué de recevoir, de la part de différentes institutions et agences, des notifications concernant les procédures de certification et d'attestation. Ses recommandations portent notamment sur les périodes de conservation des données, tenant compte des droits de recours et des nouvelles candidatures des mêmes personnes.

Deux avis de contrôle préalable ont trait à la procédure de retraite anticipée à la Commission (dossier 2006-577) et à l'OHMI (dossier 2007-575). Dans d'autres domaines, les recommandations concernent la durée de conservation des données et le droit d'accès de la personne concernée au rapport du comité chargé de décider quelles personnes ont droit à une retraite anticipée, sous réserve de certaines restrictions conformément à l'article 20, paragraphe 1, point c), du règlement. Le CEPD s'est aussi interrogé sur la nécessité de publier la liste de réserve des personnes demandant une retraite anticipée.

Enfin, dans les différents domaines de l'évaluation du personnel, des avis ont été rendus concernant une étude sur le stress au travail à l'OHMI, les conseillers spéciaux, les indemnités spéciales, la liste d'enregistrement des observateurs électoraux et l'exercice de redéploiement.

**Procédures de l'OLAF:** le CEPD a rendu douze avis concernant les procédures de l'OLAF (l'un de ces avis est un contrôle préalable proprement dit et porte sur le système de notification des fraudes, voir le point 2.3.5). Un avis (dossiers conjoints 2006-544 à 2006-547) traite du suivi judiciaire, disciplinaire, administratif ou financier. Ces quatre traitements de données à caractère personnel sont effectués au cours de la troisième phase des enquêtes de l'OLAF, dite «phase de suivi», qui vise à garantir que l'autorité communautaire et/ou les autorités nationales compétentes ont mis en œuvre les mesures recommandées par l'OLAF. De manière générale, les procédures respectent les principes inscrits dans le règlement relatif à la protection des données. Le CEPD a néanmoins formulé quelques recommandations, principalement en ce qui concerne la nécessité de certaines données introduites dans le système, l'obligation de prouver la nécessité de transfert de données et les informations fournies aux personnes concernées. Il a également demandé que la durée de conservation des données, fixée à vingt ans, soit examinée par l'OLAF lorsque celui-ci aura atteint dix années

<sup>(9)</sup> Par ailleurs, dans le cadre d'une plainte (dossier 2007-529, voir ci-après), le CEPD a formulé une autre recommandation portant sur l'équité du traitement, demandant qu'une procédure plus détaillée soit mise en place en ce qui concerne les «aspects prioritaires».



Les dossiers médicaux contiennent toujours des données sensibles.

d'existence. Le CEPD a souligné qu'il conviendra de tenir compte des recommandations qu'il a formulées dans son avis lors de la mise à jour du manuel de l'OLAF pour le traitement des données.

Un autre avis traite des enquêtes externes (dossiers 2007-047 à 2007-050 et 2007-072). Il s'agit d'enquêtes administratives menées en dehors des organes communautaires, qui visent à déceler des fraudes ou d'autres irrégularités commises par des personnes physiques ou morales et portant atteinte aux intérêts financiers des Communautés européennes. Les résultats des enquêtes externes de l'OLAF sont adressés aux autorités nationales ou communautaires compétentes à des fins de suivi judiciaire, administratif, législatif ou financier. Le CEPD a ainsi demandé à l'OLAF d'insérer une note au fichier établissant la nécessité du transfert de données à caractère personnel dans un cas précis et de garantir, à titre de règle générale, l'exercice du droit d'accès et de rectification des données à caractère personnel par les personnes concernées. À cet égard, l'OLAF doit veiller à ce que toute limitation, au titre de l'article 20 du règlement, du droit d'accès aux données personnelles et/ou du droit de les rectifier respecte le critère de nécessité appliqué au cas par cas, conformément aux dispositions de l'article 20, paragraphes 3, 4 et 5, du règlement. Il doit en outre respecter la confidentialité des dénonciateurs et des informateurs au cours des enquêtes externes qu'il effectue.

Le CEPD a également procédé au contrôle préalable des opérations de traitement effectuées par le comité de surveillance de l'OLAF (dossier 2007-0073). Ce type de traitement a pour objectif de renforcer l'indépendance de l'OLAF grâce à un contrôle régulier de la mise en œuvre de la fonction d'enquête, comme l'exige l'article 11 du règlement (CE) n° 1073/1999. Le CEPD a recommandé, entre autres, que le comité de surveillance n'ait accès au système de gestion des dossiers (en cours, clôturés et non-lieux) qu'au cas par cas. Lorsque cet accès est demandé, il convient d'insérer une note dans le fichier du système de gestion des dossiers précisant les motifs qui justifient l'octroi de l'accès. En outre, le comité de surveillance doit respecter l'article 12 du règlement pour ce qui est des personnes concernées, y compris les dénonciateurs, les témoins et les informateurs.

Le CEPD a donc analysé de manière approfondie les opérations de traitement de l'OLAF en ce qui concerne les données relatives à des suspicions, et il a, le cas échéant, formulé des recommandations. On peut citer entre autres:

- le système de notification des fraudes (2007-481);
- le pool de données en matière d'information et de renseignement et les bases de données de renseignement (dossiers conjoints 2007-027 et 2007-028);
- les dossiers d'assistance pénale (2007-203);
- le système d'information douanier (dossier 2007-177);
- le système d'information antifraude (AFIS) (dossiers conjoints 2007-084 à 2007-087);
- le service d'appel gratuit (dossier 2007-003).

**Services sociaux:** les dossiers du service social peuvent contenir des informations liées à la santé d'un fonctionnaire, domaine pour lequel le traitement des données est soumis au contrôle préalable du CEPD. Par ailleurs, les traitements effectués par ce service peuvent être destinés à évaluer des aspects de la personnalité des personnes concernées.

Le CEPD a donc rendu un certain nombre d'avis dans ce domaine. Il a notamment recommandé que l'assistant(e) social(e) qui traite les données à caractère personnel soit correctement informé(e) de l'obligation de respecter le principe énoncé à l'article 4, paragraphe 1, point c), du règlement, selon lequel les données traitées doivent être «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement». Ce principe doit être respecté en ce qui concerne les données fournies par le demandeur et les notes personnelles de l'assistant(e) social(e).

Le CEPD a ainsi maintes fois souligné dans ses avis concernant les services sociaux la très grande prudence dont doit faire preuve l'assistant(e) social(e) lorsqu'il (elle) communique avec des services externes, et ce en raison de la nature même des données transférées. Il a également précisé que le droit de rectification dans le cas des dossiers sociaux conservés par l'assistant(e) social(e) signifie que la personne concer-

née a le droit de donner son point de vue, surtout lorsque l'évaluation subjective de l'assistant(e) social(e) pourrait avoir des conséquences sur l'exercice des droits de la personne concernée.

**Contrôle des communications électroniques:** bien que le CEPD n'ait pas encore adopté de position définitive sur la question du contrôle des communications électroniques (voir le point 2.8), il a rendu plusieurs avis dans ce domaine. Deux de ces avis portent sur la procédure d'enquête à la BCE relative à l'utilisation des téléphones de service et des téléphones portables professionnels (dossiers 2004-271 et 2004-272). Ces deux avis contiennent une recommandation concernant la durée de conservation des données relatives au trafic qui ne devrait pas, en principe, excéder six mois, sauf dans certains cas particuliers. Les données relatives au trafic peuvent être traitées à des fins statistiques, à condition d'avoir été rendues anonymes.

Le CEPD a par ailleurs rendu un avis concernant le contrôle silencieux des communications professionnelles au standard de l'OHMI et au centre d'information (dossier 2007-128), effectué de manière sélective (deux ou trois fois par an), et visant notamment à évaluer la qualité du service, à améliorer la satisfaction des clients et, en fin de compte, à assurer la formation des nouveaux membres du personnel. Le CEPD a estimé que le traitement pouvait se fonder sur l'article 5, point a), du règlement, puisqu'en principe il pouvait être considéré comme nécessaire aux fins décrites, avec toutefois certaines nuances quant à la formation. Il a également souligné qu'il conviendrait d'élaborer une méthode à même de garantir l'exactitude des données.

De nombreux dossiers notifiés au CEPD concernant le suivi électronique n'ont pas été soumis à un contrôle préalable, les données étant traitées aux seules fins de la facturation et de la gestion du trafic et n'étant pas liées à des risques particuliers, à des suspicions ou à l'évaluation (voir le point 2.3.7).

(Pour ce qui est de la vidéosurveillance, voir le point 2.9.)

### 2.3.5. Principales questions soulevées dans le cadre des contrôles préalables proprement dits

En principe, le CEPD devrait rendre son avis avant qu'un traitement ne débute, afin que les droits et les libertés des personnes concernées soient garantis dès le départ. Tel est l'objet de l'article 27. Parallèlement aux dossiers de contrôle préalable a posteriori, onze dossiers de contrôle préalable proprement dit<sup>(10)</sup> ont été notifiés au CEPD en 2007. Parmi ces onze dossiers, deux ont concerné un cas d'insuffisance professionnelle et quatre l'horaire flexible.

<sup>(10)</sup> C'est-à-dire portant sur des traitements dont la mise en œuvre n'a pas encore débuté.

La Cour des comptes a mis en place une procédure applicable en cas de signes d'insuffisance professionnelle d'un membre du personnel, qui vise également à remédier à une telle situation (dossier 2006-534). L'examen du CEPD a essentiellement donné lieu à des recommandations relatives aux informations à fournir aux membres du personnel, notamment en ce qui concerne la décision concernée, la décision de mise en œuvre de la Cour concernant la protection des données, ainsi que la fixation de délais de conservation des données. Les recommandations formulées sur le dossier notifié par le Parlement européen (2006-572) ont, quant à elles, porté sur plusieurs points, parmi lesquels la conservation des données concernant des procédures d'amélioration menées à leur terme ou interrompues, ou le traitement de données relatives à la santé dans ce contexte.

Les **systèmes de gestion du temps de travail** ont fait l'objet d'une grande attention en 2007. La Commission a présenté au CEPD une notification générale (dossier 2007-63) concernant le module de gestion du temps du Sysper 2 (système de gestion du personnel), qui gère notamment les données de l'horaire flexible; cette notification a été suivie de deux notifications portant sur les systèmes d'horaire flexible spécifiques de deux DG (dossier 2007-218 sur l'horaire flexible à la DG Société de l'information et médias et dossier 2007-680 sur l'horaire flexible à la DG Agriculture et développement rural), établies à partir de la notification de référence. Ces dossiers remplissaient les conditions requises en vue d'un contrôle préalable, conformément à l'article 27, paragraphe 2, point a) (données relatives à la santé), et à l'article 27, paragraphe 2, point b) (traitement destiné à évaluer la compétence, le rendement et le comportement au travail du personnel).

Le contrôle préalable proprement dit dont a fait l'objet le module de gestion du temps de la Commission n'a porté que sur son volet «**horaire flexible**» et a donné lieu, entre autres, à des recommandations concernant l'utilisation du numéro personnel des agents, pour assurer la cohérence du système, la mention du caractère obligatoire ou facultatif des données collectées auprès du personnel et un affichage séparé s'agissant du crédit temps total.

La DG Société de l'information et médias a ajouté à l'application «flexitime» une composante supplémentaire et de poids sous la forme d'une puce RFID intégrée dans le badge personnel nécessaire au pointage. L'introduction d'une technologie de cette nature dans un système d'horaire flexible augmente les risques spécifiques déjà inhérents au système. Dans ses conclusions, le CEPD a demandé que plusieurs modifications soient apportées au système prévu en ce qui concerne les aspects de sécurité, en mettant en place une solution provisoire, ainsi qu'en ce qui concerne le libellé de la déclaration relative au respect de la vie privée, certaines mesures organisationnelles et les personnes concernées.

Pour ce qui est du système d'horaire flexible spécifique de la DG Agriculture et développement rural, le CEPD a jugé que la notification présentée était contraire au règlement

(CE) n° 45/2001, l'objectif visé (donner à plusieurs personnes au sein d'une unité — et non pas au seul chef d'unité — la possibilité d'identifier l'absence d'un membre du personnel afin de le remplacer dans les meilleurs délais) pouvant être atteint en utilisant d'autres moyens moins intrusifs. En outre, selon le CEPD, l'objectif poursuivi par la DG Agriculture et développement rural ne peut être atteint au moyen du système d'horaire flexible proposé.

Le quatrième dossier relatif à la gestion du temps de travail a été présenté par la Fondation européenne pour la formation (dossier 2007-209). Le système d'enregistrement du temps de travail a pour objet d'informer l'administration de l'ETF du temps que les membres du personnel et les équipes en place consacrent à la réalisation des différentes tâches et des divers projets. Les principales recommandations ont concerné la qualité des données, très difficile à garantir en raison de la manière dont le système a été conçu, ainsi que la limitation de la finalité, en vertu de laquelle les informations doivent être utilisées non à des fins d'évaluation du personnel, mais uniquement à des fins de gestion d'un projet.

Un autre avis en vue d'un contrôle préalable proprement dit a été publié sur une question relative à la gestion du temps de travail, à savoir le dossier notifié par la BEI sur les dossiers médicaux et la gestion du temps (dossier 2007-373). Dans un premier temps, le dossier a été envoyé au CEPD en vue d'une consultation quant à la nécessité d'un contrôle préalable, étant donné que deux avis avaient été précédemment rendus sur ces questions (dossier 2005-396 sur les dossiers médicaux et dossier 2004-306 sur la gestion du temps) et que l'objectif de la BEI était que le médecin du centre de médecine du travail ait accès à toutes les données relatives aux absences pour maladie sans certificat contenues dans le système de gestion du temps de travail. C'est la première fois que le CEPD a été amené à publier un nouvel avis sur la base de modifications apportées à l'objet de dossiers ayant déjà été soumis au contrôle préalable.

Dans son avis, le CEPD a estimé que la BEI enfreindrait certaines dispositions du règlement (licéité du traitement des données, principe de la qualité des données, traitement portant sur des catégories particulières de données) si elle ne veillait pas à demander aux membres du personnel d'accepter librement et indubitablement que le médecin du centre de médecine du travail ait accès aux données concernant leurs absences pour maladie sans certificat. Lorsqu'elle recueille ce consentement, la BEI doit s'assurer que le membre du personnel sait qu'il peut refuser son consentement ou le retirer à tout moment ultérieur, sans la moindre justification et sans être pénalisé. Elle doit également clairement faire savoir que ces informations ne seront utilisées qu'à des fins de prévention.

Parmi les autres dossiers de contrôle préalable a posteriori, le CEPD met en évidence les suivants:

— le dossier notifié par EPSO (2007-88) sur l'évaluation de la capacité à travailler dans une troisième langue, qui



Les systèmes de gestion du temps contiennent des données sur le comportement et d'autres aspects de la personnalité.

- a donné lieu à une recommandation concernant les corrections automatiques effectuées par les sous-traitants;
- le dossier notifié par le Médiateur européen (2007-134) sur la gestion des congés, qui a donné lieu à des recommandations concernant les données relatives à la santé et l'information de la personne concernée;
- le dossier notifié par la BCE (2007-371) sur les règles d'habilitation (traitement de données effectué par la BCE dans le cadre de l'application des procédures d'habilitation de sécurité afin de déterminer si une personne remplit les conditions pour recevoir une habilitation de sécurité), qui met l'accent sur la nécessité d'éviter des données excessives;
- le dossier notifié par l'OLAF sur le système de notification des fraudes (système d'information en ligne que l'OLAF a mis à la disposition du public pour faciliter la collecte d'informations utilisées dans le cadre de la lutte contre la fraude, la corruption et d'autres activités illégales préjudiciables aux intérêts financiers de la Communauté), qui met l'accent sur deux questions essentielles: l'information des personnes qui sont concernées par les informations reçues et la protection des informateurs et des dénonciateurs.

### 2.3.6. Consultations quant à la nécessité d'un contrôle préalable

Au cours de l'année 2007, le nombre de consultations quant à la nécessité d'un contrôle préalable par le CEPD a considérablement augmenté, passant de quinze en 2006 à vingt en 2007. Plusieurs dossiers susmentionnés ont dans un premier temps fait l'objet d'une consultation, à savoir notamment les dossiers concernant les dossiers médicaux et la gestion du temps, le système d'horaire flexible de la DG Société de l'information et médias, les données traitées par les conseillers sociaux et les exercices de redéploiement.

D'autres dossiers déclarés soumis au contrôle préalable, comme ceux concernant le «prix annuel», les «enquêtes de sécurité», les «consultants indépendants», l'utilisation des «listes de réserve établies par EPSO», l'«instrument de rapprochement dans le cadre d'un audit» et la «base de données des experts de l'EFSA», n'ont pas encore été officiellement notifiés au CEPD depuis que celui-ci a indiqué qu'il était nécessaire de les soumettre à un contrôle préalable.

Le CEPD a estimé que le traitement de données concernant des «personnes politiquement exposées» au sein de la BEI devait être soumis au contrôle préalable, car il porte sur des données relatives à des condamnations pénales ou à des soupçons d'infractions pénales.

Le dossier concernant les règles applicables à l'accès des enfants des membres du personnel aux bâtiments de l'OHMI constitue un cas particulier puisque, alors que le CEPD avait initialement déclaré ce dossier soumis au contrôle préalable, il en a ensuite été dessaisi. En effet, l'OHMI a modifié ces règles de sorte qu'elles ne donnent plus lieu au traitement de données à caractère personnel.

Le CEPD a conclu que le traitement des données relatives à la gestion de l'accès à l'internet au sein de la Cour de justice n'était pas soumis au contrôle préalable. En effet, ce traitement ne visait pas à évaluer le comportement des personnes et n'entraînait pas de violation de la confidentialité des communications.

De la même manière, il a été conclu que le traitement des données relatives à la téléphonie au sein du Conseil n'était pas soumis au contrôle préalable, car il n'entraînait pas de violation de la confidentialité des communications.

Un autre avis intéressant en la matière a été rendu sur le dossier notifié par la Cour de justice concernant le système de messagerie électronique. Ce système n'est pas soumis au contrôle préalable étant donné qu'aucun mécanisme de surveillance régulière ou aléatoire n'a été mis en place afin de contrôler l'utilisation abusive du courrier électronique. En outre, aucun traitement n'est destiné à évaluer des aspects de la personnalité d'une personne, tels que sa compétence, son rendement ou son comportement.

Enfin, bien que le traitement des données relatives à l'organisation de déplacements, effectué au sein du Conseil, puisse concerner des données relatives à la santé, le CEPD a conclu

qu'il n'était pas soumis au contrôle préalable. En effet, il apparaît clairement que ce traitement ne vise pas à traiter des données médicales, ce type de données n'étant traité que dans de rares cas et avec le consentement de la personne concernée.

### 2.3.7. Notifications non soumises au contrôle préalable

En 2007, le CEPD a également examiné trente et un dossiers pour lesquels il a conclu qu'ils n'étaient pas soumis au contrôle préalable (soit 23,48 % des dossiers sur lesquels il a rendu un avis officiel). Il est parvenu à ces conclusions à l'issue d'un examen approfondi des notifications.

Néanmoins, ces examens ont, le plus souvent, donné lieu à des recommandations du CEPD. Onze de ces dossiers concernent le contrôle des communications électroniques, deux l'horaire flexible et quatre le contrôle de l'accès, les autres portant soit sur des questions relatives au personnel (classement initial, cartes d'identité, demandes concernant l'exercice d'activités extérieures, renouvellement de contrats, règles relatives aux opérations d'initiés) soit sur différentes autres questions telles que les accréditations ou des enquêtes du DPD ouvertes par l'OLAF.

En ce qui concerne les dossiers relatifs au **contrôle des communications électroniques**, la plupart des notifications<sup>(11)</sup> en vue d'un contrôle préalable ont été adressées au CEPD sur la base de l'article 27, paragraphe 1, du règlement.

Il convient de rappeler que les communications électroniques peuvent être soumises au contrôle préalable du CEPD dans deux principaux cas de figure:

- L'article 27, paragraphe 1, du règlement soumet au contrôle préalable tous les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités. Le chapitre IV du règlement contient une disposition spécifique sur la confidentialité des communications (article 36). En cas de violation de la confidentialité des communications, il peut exister un risque particulier au regard des droits et libertés des personnes concernées; le traitement concerné est donc soumis au contrôle préalable du CEPD.
- L'article 27, paragraphe 2, contient une liste non exhaustive des traitements susceptibles de présenter de tels risques. Cette liste comprend entre autres:

- les traitements de données relatives à des suspicions, des infractions ou des mesures de sûreté [article 27, paragraphe 2, point a)];
- les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement [article 27, paragraphe 2, point b)].

Lorsqu'un mécanisme est mis en place pour surveiller un réseau de communication aux fins visées à l'article 27, paragraphe 2, point a) et/ou point b), du règlement, les traitements doivent être soumis au contrôle préalable du CEPD.

Cela signifie que tous les systèmes de communication électronique ne sont pas nécessairement soumis au contrôle préalable. En fait, dès lors qu'il n'est pas porté atteinte à la confidentialité des communications et que l'infrastructure informatique n'est pas utilisée pour surveiller le comportement du personnel, il n'y a, bien souvent, pas de raison de soumettre les systèmes de communications électroniques au contrôle préalable.

Cela dit, le CEPD a néanmoins formulé des recommandations concernant les périodes de conservation des données relatives au trafic et à la facturation, conformément à l'article 37, paragraphe 2, du règlement, et les informations à communiquer aux personnes concernées.

Pour ce qui est du **contrôle de l'accès**, trois notifications<sup>(12)</sup> ont été présentées au titre de l'article 27, paragraphe 2, point b). Après avoir examiné ces notifications, le CEPD a conclu qu'aucun des traitements en question ne portait sur l'évaluation d'aspects de la personnalité. Il a toutefois formulé des recommandations concernant la finalité exacte du traitement. La quatrième notification<sup>(13)</sup> a été présentée au titre de l'article 27, paragraphe 2, points a) et b), mais il est apparu que ces deux dispositions n'étaient pas applicables à ce dossier. En effet, l'article 27, paragraphe 2, point a), ne s'applique que dans des circonstances exceptionnelles et l'article 27, paragraphe 2, point d), n'était pas applicable, car la liste des exclusions n'avait pas été établie par le responsable du traitement.

Le CEPD a conclu que les deux dossiers relatifs à la **gestion du temps de travail**<sup>(14)</sup> n'étaient pas soumis au contrôle préalable, étant donné qu'ils ne concernaient pas l'évaluation du personnel, mais plutôt l'évaluation des activités de l'OLAF ou du CCR. Le traitement d'informations aux fins du suivi des activités d'une institution de l'UE, dans le but de mieux prévoir l'affectation des ressources, ne relève pas des critères énoncés à l'article 27, paragraphe 2, du règlement. Le dossier notifié par le CCR a donné lieu à de nombreuses recommandations relatives à la limitation de la finalité, à la qualité des données, aux informations à com-

<sup>(11)</sup> Notifications concernant un système de messagerie électronique ou la téléphonie (dossiers 2006-507 et 2006-508 du CESE et du CdR), l'infrastructure liée aux téléphones et aux télécopieurs, les statistiques internet, une base de données des appels téléphoniques, la facturation des appels téléphoniques (dossiers 2007-358, 2007-359, 2007-367 et 2007-374 de la Commission), la téléphonie fixe et la téléphonie mobile (dossiers 2007-438 et 2007-439 de la Cour de justice), un registre d'appels téléphoniques (dossier 2004-302 de la BEI) et la facturation de l'utilisation de téléphones mobiles de service à des fins privées (dossier 2007-204 de l'OLAF).

<sup>(12)</sup> Commission (dossiers 2007-375, 2007-376 et 2007-381).

<sup>(13)</sup> Commission (dossier 2004-235).

<sup>(14)</sup> Système de comptabilité du temps du CCR de la Commission (dossier 2007-503) et système de gestion du temps de l'OLAF (dossier 2007-300).

muniquer aux personnes concernées et à la période de conservation des données.

### 2.3.8. Suivi des avis relatifs aux contrôles préalables

Lorsque le CEPD rend un avis relatif au contrôle préalable, cet avis est habituellement assorti d'une série de **recommandations** qui doivent être prises en considération pour que le traitement soit conforme au règlement. Des recommandations sont également formulées lorsque le CEPD examine un dossier afin de décider de la nécessité d'un contrôle préalable et que certains aspects essentiels semblent nécessiter des rectifications.

Si le responsable du traitement ne respecte pas ces recommandations, le CEPD peut exercer les pouvoirs qui lui sont conférés en vertu de l'article 47 du règlement. Il peut en particulier saisir l'institution ou l'organe communautaire concerné et prendre des mesures complémentaires afin de garantir le respect des recommandations. Si les décisions du CEPD ne sont pas respectées, celui-ci a le droit de saisir la Cour de justice dans les conditions prévues par le traité CE.

Tous les cas de contrôle préalable ont abouti à des recommandations. Comme expliqué plus haut (voir les points 2.3.4 et 2.3.5), la plupart des recommandations concernent les informations communiquées aux personnes concernées, les périodes de conservation des données, la limitation de la finalité et les droits d'accès et de rectification. Les institutions et organes sont disposés à suivre ces recommandations et, à ce jour, il n'a pas été nécessaire de prendre de décisions d'exécution. Le temps nécessaire à la mise en œuvre de ces mesures diffère selon les cas. Depuis juin 2006, le CEPD demande, dans une lettre formelle transmise avec ses avis, que l'institution concernée l'informe, dans un délai de trois mois, des mesures adoptées pour mettre en œuvre les recommandations formulées.

Au cours de l'année 2007, le CEPD a clos trente-huit dossiers, soit plus de deux fois plus qu'en 2006, ce qui s'explique de toute évidence par le suivi systématique de toutes les recommandations.

### 2.3.9. Conclusions et perspectives

Il apparaît clairement que la conduite de contrôles préalables, tant «proprement dits» qu'«a posteriori», est restée une activité importante du CEPD dans le cadre de sa mission de contrôle. Dès le début, il a été décidé, de manière stratégique, que l'application a posteriori de l'article 27 du règlement serait un excellent moyen de contrôler le traitement des données à caractère personnel au sein des institutions et organes de l'UE dans les domaines comportant le plus de risques, ce qui a en effet été le cas.

Les conclusions pour 2007 peuvent être résumées comme suit:

- l'échéance fixée au «printemps 2007» a entraîné une augmentation considérable des notifications envoyées par nombre des DPD, en particulier pendant le premier semestre de l'année, au cours duquel plus de 42 % du nombre total de notifications (soit 132 sur les 313 envoyées entre 2004 et le 31 décembre 2007) ont été reçues;
- cette évolution a exercé une pression importante sur l'équipe de contrôle du CEPD, mais les résultats enregistrés ont été très satisfaisants étant donné que le nombre élevé d'avis élaborés n'a pas eu d'incidence sur leur délai d'élaboration (y compris les jours de prolongation) et que le respect de la qualité a été assuré;
- il reste encore beaucoup à faire pour réduire les temps de réponse des institutions et organes communautaires aux demandes d'informations complémentaires du CEPD;
- aucun domaine prioritaire précis n'ayant été défini pour les contrôles a posteriori, l'éventail des questions examinées par le CEPD s'est considérablement élargi (gestion du temps de travail, dossiers notifiés par l'OLAF, traitement interinstitutionnel, etc.);
- comme l'année précédente, les avis rendus sur deux dossiers ont conclu que le règlement avait été enfreint et qu'il était nécessaire d'introduire des modifications importantes pour faire respecter les règles applicables en matière de protection des données;
- les recommandations ont continué de porter essentiellement sur la conservation des données, le droit d'information et le droit d'accès.

À l'avenir, les efforts déployés se concentreront sur les points suivants:

- les institutions devraient achever la mise au point de leur processus de notification a posteriori et les organes devraient réaliser un important pas en avant en ce sens en 2008;
- les recommandations du CEPD continueront de faire l'objet d'un suivi systématique grâce aux informations communiquées par le responsable du traitement, et ce suivi sera associé à des vérifications sur place. Il s'agira également de s'assurer de la mise en œuvre pleine et entière du processus de notification aux DPD et du respect total de l'obligation de notifier au CEPD les dossiers de contrôle préalable proprement dit avant le début du traitement;
- certains domaines, tels que la vidéosurveillance, feront l'objet d'une nouvelle approche, fondée sur la définition de normes et la présentation d'une notification en vue d'un contrôle préalable seulement en cas de non-respect;

- les critères mis au point à ce jour seront résumés par catégorie afin de veiller à la cohérence de tous les avis rendus et de donner aux institutions et organes des orientations en vue de la mise en œuvre des règles en matière de protection de données.

## 2.4. Plaintes

### 2.4.1. Introduction

L'article 41, paragraphe 2, du règlement prévoit que le CEPD «est chargé de surveiller et d'assurer l'application des dispositions du présent règlement et de tout autre acte communautaire concernant la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par une institution ou un organe communautaire». Cette surveillance prend notamment la forme de l'examen de plaintes, prévu à l'article 46, point a) <sup>(15)</sup>.

Conformément aux articles 32 et 33 du règlement, toute personne physique peut présenter une plainte au CEPD indépendamment de sa nationalité ou de son lieu de résidence <sup>(16)</sup>. Les membres du personnel des institutions et organes de l'UE visés au statut peuvent également soumettre une plainte en vertu de l'article 90 ter dudit statut <sup>(17)</sup>.

Les plaintes ne sont recevables que si elles émanent d'une personne physique et concernent la violation des règles de protection des données par une institution ou un organe de l'UE lors du traitement de données à caractère personnel dans le cadre de l'exercice d'activités qui relèvent en tout ou en partie du champ d'application de la législation communautaire. Ainsi qu'il est précisé ci-après, un certain nombre de plaintes présentées au CEPD ont été déclarées irrecevables, car elles ne relevaient pas du domaine de compétence du CEPD.

Lorsque le CEPD reçoit une plainte, il envoie un accusé de réception à l'auteur de la plainte, sans se prononcer sur sa recevabilité, sauf dans le cas où la plainte est manifestement irrecevable, sans qu'il soit nécessaire de procéder à un examen complémentaire. Le CEPD demande aussi à l'auteur de la plainte de l'informer d'éventuelles autres actions engagées

<sup>(15)</sup> Selon l'article 46, point a), le CEPD «entend et examine les réclamations et informe la personne concernée des résultats de son examen dans un délai raisonnable».

<sup>(16)</sup> Selon l'article 32, paragraphe 2, «[...] toute personne concernée peut présenter une réclamation au Contrôleur européen de la protection des données si elle estime que les droits qui lui sont reconnus à l'article 286 du traité ont été violés à la suite du traitement de données à caractère personnel la concernant, effectué par une institution ou un organe communautaire». En vertu de l'article 33, «toute personne employée par une institution ou un organe communautaire peut présenter une réclamation au Contrôleur européen de la protection des données pour une violation alléguée des dispositions du [...] règlement [(CE) n° 45/2001] [...], sans passer par les voies officielles».

<sup>(17)</sup> Toute personne visée au statut des fonctionnaires peut soumettre au CEPD une demande ou une plainte au sens de l'article 90, paragraphes 1 et 2, dans le cadre de ses compétences.

devant une juridiction nationale, la Cour de justice ou auprès du Médiateur européen (pendantes ou non).

Si la plainte est recevable, le CEPD procède à une enquête, notamment en contactant l'institution/l'organe concernés ou en demandant des renseignements complémentaires à l'auteur de la plainte. Le CEPD est habilité à obtenir du responsable du traitement ou de l'institution/l'organe concernés l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires aux besoins de l'enquête. Il peut également obtenir l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution/l'organe exerce ses activités.

En cas de violation supposée de la législation régissant la protection des données, le CEPD peut saisir le responsable du traitement concerné et formuler des propositions tendant à remédier à cette violation ou à améliorer la protection des personnes concernées. Dans ce cas, le CEPD peut:

- ordonner au responsable du traitement de satisfaire les demandes d'exercice de certains droits présentées par la personne concernée;
- adresser un avertissement ou une admonestation au responsable du traitement;
- ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données;
- interdire le traitement;
- saisir l'institution communautaire concernée ou le Parlement européen, le Conseil ou la Commission;
- saisir la Cour de justice <sup>(18)</sup>.

Lorsque la décision suppose l'adoption de mesures par l'institution/l'organe, le CEPD met en place un suivi avec l'institution/l'organe concernés.

En 2007, le CEPD a reçu 65 plaintes. Sur ces 65 plaintes, 29 ont été déclarées recevables et ont fait l'objet d'un examen plus poussé par le CEPD. Certaines d'entre elles sont brièvement présentées ci-après.

### 2.4.2. Plaintes déclarées recevables

Collecte de données excessives relatives à des visiteurs

Le CEPD a reçu une plainte d'une personne venue visiter la Commission européenne avec un groupe, concernant la communication du numéro de passeport et de la date de naissance de tous les membres du groupe (dossier 2006-0578). Après enquête, le CEPD a conclu que cette pratique était excessive puisqu'elle n'était pas conforme au principe du caractère adéquat des données prévu à l'article 4, paragraphe 1, points b) et c). À la suite de l'enquête menée par le CEPD, cette pratique a cessé et le CEPD a estimé que la question était réglée. Le CEPD a mis à profit cette plainte pour rappeler à la Commission son obligation de fournir

<sup>(18)</sup> Voir l'article 47, paragraphe 1, du règlement (CE) n° 45/2001.

certaines informations aux responsables ou aux personnes chargées de la coordination des groupes, afin de garantir un traitement loyal des données.

Une autre plainte reçue a concerné le traitement de données à caractère personnel par le Parlement européen dans le cadre de la participation à une audition (dossier 2007-0430). Il a été demandé à l'auteur de la plainte de fournir certains détails en vue de sa participation à cette audition, tels que son nom et sa date de naissance. Lorsque cette personne s'est rendue à l'audition, elle a été choquée de constater que la date de naissance de chaque participant était divulguée à tous, puisqu'elle figurait sur la liste des délégués distribuée lors de l'audition. Après enquête du CEPD, il a été conclu que ces données étaient nécessaires à la délivrance de badges par le service de sécurité du Parlement européen, mais que, en effet, ces données n'auraient pas nécessairement dû être diffusées à l'ensemble des participants et que cette question fera l'objet d'un examen approfondi à l'avenir.

### Accès aux données

Un jeune expert travaillant au sein d'une délégation de la Commission européenne a adressé au CEPD une plainte concernant l'accès limité qui lui a été donné à son dossier personnel, en violation de l'article 13 du règlement (dossier 2007-0127). L'auteur de la plainte s'est également indigné que la Commission ait contacté ses précédents employeurs sans son consentement, ne l'informant donc pas des sources des données, et que la DG Relations extérieures ait transféré des données à caractère personnel le concernant à la délégation de la Commission pour laquelle il travaillait.

Après avoir examiné les faits, le CEPD a conclu que certaines limitations du droit d'accès étaient justifiées sur la base de l'article 20, paragraphe 1, point c), notamment dans la mesure où elles étaient nécessaires pour garantir la protection des précédents employeurs de l'expert. En ce qui concerne le fait que la Commission ait contacté les précédents employeurs de l'auteur de la plainte sans son consentement, le CEPD a conclu que, étant donné que l'auteur de la plainte avait lui-même fourni des informations complètes concernant ses précédents employeurs et signé un formulaire de demande dans lequel il déclarait que les informations communiquées étaient exactes, complètes et correctes, il était raisonnable de penser que l'employeur pouvait contacter les précédents employeurs de l'auteur de la plainte afin de confirmer ses déclarations. Enfin, en ce qui concerne le transfert de données de la DG Relations extérieures à la délégation de la Commission, le CEPD a conclu que ce transfert était nécessaire à l'exécution légitime des missions de la délégation de la Commission, conformément à l'article 7, point 1), du règlement.

L'auteur de la plainte a également saisi le Médiateur européen d'une plainte. Le CEPD a donc transmis le résultat de son enquête au Médiateur afin d'éviter les doubles emplois.

Une autre plainte a été envoyée par un fonctionnaire de la Commission, qui a fait valoir son droit d'accès au procès-verbal (PV) établi à la suite de l'entretien qu'il a passé pour obtenir son poste actuel (dossier 2007-0250). Dans ce cas, par «droit d'accès», il faut entendre l'accès aux données à caractère personnel concernant l'auteur de la plainte et figurant dans le PV élaboré par le jury. Après enquête, le CEPD a conclu qu'aucun PV n'avait été établi et que, par conséquent, aucune donnée à caractère personnel n'avait été enregistrée dans le cadre de l'évaluation de l'entretien oral. Le droit d'accès prévu à l'article 13 du règlement ne pouvait donc pas s'appliquer. Le CEPD a clos le dossier en soulignant que l'enregistrement de l'évaluation finale d'un test/entretien oral constituait un principe général de bonne administration.

Une plainte a été présentée contre la Commission concernant le droit d'accès aux documents préparatoires relatifs à l'attribution des points de priorité (dans le cadre de la procédure de promotion) (dossier 2007-0529). L'accès à ces données a été refusé sur la base du statut, compte tenu de la confidentialité des travaux du jury.

Le CEPD est parvenu à la conclusion que l'article 6 de l'annexe III du statut (secret des travaux du jury) devait être interprété en liaison avec l'article 20, paragraphe 1, point c), du règlement. L'indépendance et la liberté des directeurs ne sont pas menacées par le droit d'accès de la personne concernée, mais les données en question ne devraient pas pouvoir être associées à une personne identifiable. Toutefois, cette conclusion n'a pas pu être appliquée à la plainte concernée, étant donné que les documents avaient été détruits et que la Commission n'était donc pas en mesure de les rendre accessibles. En conséquence, le CEPD a demandé l'établissement d'une nouvelle note détaillée concernant l'attribution et la gestion des points de priorité afin de satisfaire à l'article 4, paragraphe 1, point a) (traitement loyal), et à l'article 12 (informations à communiquer) du règlement.

Une plainte a été présentée contre la Cour des comptes européenne s'agissant du droit d'accès d'une personne, en vertu de l'article 13, aux évaluations du personnel et aux documents à l'appui des rapports de notation, ainsi qu'aux éventuels dossiers personnels secondaires (dossier 2006-597).

Après avoir demandé des éclaircissements à la fois au responsable du traitement et à l'auteur de la plainte, le CEPD a conclu que la procédure d'évaluation au sein de la Cour des comptes (ayant fait l'objet d'un contrôle préalable par le CEPD dans le dossier 2005-0152) n'exigeait pas de disposer de documents étayant les déclarations figurant dans les rapports de notation. En outre, le CEPD n'a pas trouvé de preuve de l'existence de dossiers personnels secondaires. Enfin, s'agissant de la demande de verrouillage des données, le CEPD a estimé qu'aucune des conditions prévues à l'article 15 du règlement pour obtenir un verrouillage n'était remplie dans ce dossier.

### Transmission et copie de courriers électroniques

Une plainte contre l'OLAF a été reçue concernant un courrier électronique que l'auteur de la plainte avait adressé personnellement à un membre du personnel de l'OLAF et que celui-ci a transmis à son chef d'unité et à l'adjoint du chef d'unité (dossier 2007-0188). Le CEPD a conclu que, étant donné que rien n'indiquait dans ce courrier électronique qu'il s'agissait d'un message personnel, l'agent de l'OLAF en question l'a traité conformément aux règles internes en vigueur au sein de l'Office. En conséquence, il n'y a pas eu de violation du règlement liée à la compétence des destinataires elle-même.

L'auteur de la plainte s'est également plaint du fait que la réponse reçue de la part de l'OLAF avait été transmise en copie à un grand nombre de personnes, en violation de l'article 7, point 1), du règlement. Le CEPD a reconnu que l'article 7, point 1), autorise le transfert de certaines données si elles sont nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire. Néanmoins, il a jugé que, dans le dossier en question, ce transfert n'était pas clairement justifié pour toutes les personnes ayant reçu une copie du message. En outre, tout transfert doit respecter les autres dispositions du règlement et, en particulier, celle qui prévoit que la personne concernée doit être informée des destinataires et des catégories de destinataires des données [article 11, paragraphe 1, point c)], ce qui n'a pas été le cas.

Le CEPD examine actuellement avec l'OLAF des moyens d'éviter que ce type de situation ne se reproduise.

### Obligation de fournir des informations concernant sa carte de crédit

Deux membres du personnel du Parlement européen ont présenté une plainte au CEPD concernant l'obligation de fournir son numéro de carte de crédit personnelle ou professionnelle pour confirmer la réservation d'une mission (dossier 2007-0338). Après enquête du CEPD, il est apparu que ni le Parlement ni l'agence de voyages accréditée n'exigeaient de numéro de carte de crédit pour procéder aux réservations d'hôtel. Néanmoins, les hôtels demandent un numéro de carte de crédit pour confirmer une réservation. Les seuls cas où le Parlement exige un numéro de carte sont ceux où le membre du personnel ne peut réserver une chambre dans la limite des plafonds fixés et qu'il doit présenter un formulaire de réservation indiquant la somme requise par l'agence de voyages, sur lequel figure également le numéro de sa carte de crédit. Néanmoins, depuis lors, le Parlement a supprimé du formulaire de réservation la rubrique relative au numéro de carte de crédit.

L'utilisation de la carte de crédit professionnelle relève, quant à elle, du choix personnel de chaque membre du personnel. En conséquence, tout traitement de données à caractère personnel relatives à une carte de crédit professionnelle se

fonde sur le consentement sans équivoque du membre du personnel et est légitime en vertu de l'article 5, point d), du règlement.

### Traitement des données sensibles

Un membre du personnel de la BCE a adressé au CEPD une plainte dans laquelle il affirmait que des données relatives à la santé avaient fait l'objet d'un traitement incorrect dans le cadre de la gestion des congés de maladie (dossier 2007-0299). L'auteur de la plainte estimait que cette catégorie particulière de données à caractère personnel, au sens de l'article 10, paragraphe 1, du règlement, avait été traitée sans que la nécessité de ce traitement soit suffisamment étayée en vertu de l'article 10, paragraphe 2, point b). Après avoir examiné les faits, le CEPD a conclu que la BCE avait le droit de faire valoir l'exception prévue à l'article 10, paragraphe 2, point b). Cette conclusion se fonde sur le fait que le traitement était nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en vertu du droit du travail applicable.

### Droit de rectification

À la fin de 2006, une plainte concernant le droit de rectification d'un fonctionnaire de la Commission était encore en cours d'examen (dossier 2006-0436). En 2007, le CEPD a reçu la confirmation qu'une solution temporaire avait été mise en place pour permettre au demandeur de compléter les données à caractère personnel le concernant dans son historique de carrière figurant dans Sysper 2. La Commission a également expliqué pourquoi le verrouillage des données à caractère personnel concernant l'auteur de la plainte aurait entraîné l'interruption de tous les traitements de données concernant le demandeur dans Sysper 2, par exemple le versement de son salaire. Le CEPD a clos le dossier de plainte, mais a ouvert un nouveau dossier afin de donner suite aux explications techniques fournies concernant les difficultés rencontrées par la Commission pour rectifier et verrouiller les données à caractère personnel dans la base de données de Sysper 2.

Une autre plainte a été envoyée par une personne déclarant que le terme «invalidité» apparaissait sur tous ses bulletins de pension depuis le 9 novembre 2006. La divulgation de ces données relatives à sa santé l'a exposée à d'importants désagréments dans ses relations avec trois banques. Après que cette plainte a été présentée au CEPD, la DG Personnel et administration a supprimé le terme «invalidité» des bulletins de pension de la personne concernée.

### Obligation d'information

Dans une plainte présentée contre l'OLAF (dossier 2007-0029), l'auteur de la plainte a déclaré que des données le concernant, mais n'ayant pas été collectées auprès de lui,

avaient été collectées, conservées et transférées à des tiers dans le cadre d'un rapport final de l'OLAF, sans qu'il en soit informé (article 12 du règlement). Il fondait également sa plainte sur l'article 13 du règlement, car, ayant demandé à l'OLAF de lui donner accès aux données le concernant, il avait reçu une copie du rapport final de l'OLAF où toutes les données à caractère personnel avaient été supprimées, y compris celles le concernant. Par ailleurs, l'auteur de la plainte a déclaré qu'il estimait que le rapport final de l'OLAF donnait une image partielle et tendancieuse de son comportement et qu'il souhaitait donc exercer son droit de rectification (article 14 du règlement). Après avoir examiné ce dossier, le CEPD a noté que l'OLAF n'avait pas respecté les obligations qui lui incombent en vertu des articles 11 et 12 du règlement. En outre, le CEPD a jugé que l'auteur de la plainte aurait dû recevoir une copie du rapport final sur laquelle apparaissent tous les traitements de données à caractère personnel le concernant, afin de satisfaire à l'article 13 du règlement (il convenait d'éviter la suppression des passages concernant ses données à caractère personnel). Enfin, le CEPD a indiqué qu'il évaluerait la demande de rectification introduite par l'auteur de la plainte une fois que l'accès aux données le concernant lui aura été accordé, s'il maintient sa demande.

### Présentation d'un dossier dans le rapport annuel 2005

Le 1<sup>er</sup> juillet 2005, le CEPD a reçu une plainte contre l'OLAF soulevant plusieurs questions relevant du règlement, notamment le traitement déloyal de données à caractère personnel et le transfert de données erronées concernant l'auteur de la plainte par l'OLAF, dans le cadre d'une enquête concernant sa participation supposée à une affaire de corruption, en 2002 et au début de 2004 (dossier 2005-0190).

Le 1<sup>er</sup> décembre 2005, le CEPD adjoint a adopté une décision concernant cette plainte. Il a certes reconnu que le CEPD était compétent pour entendre cette plainte, dans la mesure où elle soulève des questions relevant du règlement (CE) n° 45/2001, mais il a conclu que le CEPD n'était pas en mesure de prendre d'autres mesures, qui modifieraient la situation à l'avantage de l'auteur de la plainte. Ce dossier a été brièvement évoqué dans le rapport annuel 2005.

En 2006, l'auteur de la plainte a saisi le Médiateur européen d'une plainte concernant la manière dont sa plainte a été traitée. Dans une deuxième plainte, il a également élevé des objections contre la brève présentation de son dossier dans le rapport annuel 2005, affirmant qu'elle était incorrecte et prématurée. S'agissant de la deuxième plainte, le CEPD a accepté de fournir une mise à jour appropriée du dossier, comprenant une description correcte et complète du dossier de l'auteur de la plainte, telle qu'elle apparaît ci-dessus. La première plainte était encore examinée par le Médiateur au début de 2008.

### 2.4.3. Plaintes déclarées irrecevables: principaux motifs d'irrecevabilité

Sur les 65 plaintes reçues en 2007, 36 ont été déclarées irrecevables car ne relevant pas du domaine de compétence du CEPD. Dans leur grande majorité, ces plaintes ne concernaient pas le traitement de données à caractère personnel par une institution ou un organe communautaire, mais portaient exclusivement sur un traitement au niveau national. Dans certaines de ces plaintes, il était demandé au CEPD de réexaminer une position prise par une autorité nationale compétente en matière de protection des données, ce qui ne relève pas de son mandat. Dans ce cas, les auteurs des plaintes ont été informés que la Commission européenne serait compétente au cas où un État membre n'appliquerait pas de manière correcte les dispositions de la directive 95/46/CE.

### 2.4.4. Collaboration avec le Médiateur européen

Conformément à l'article 195 du traité CE, le Médiateur européen est habilité à recevoir les plaintes relatives à des cas de mauvaise administration dans l'action des institutions ou organes communautaires. Le Médiateur et le CEPD ont des compétences qui se chevauchent dans le cadre du traitement des plaintes dans la mesure où les cas de mauvaise administration peuvent concerner le traitement de données à caractère personnel. Par conséquent, les plaintes dont le Médiateur est saisi peuvent porter sur des questions liées à la protection des données. De même, les plaintes présentées au CEPD peuvent concerner des plaintes qui ont déjà, en tout ou en partie, fait l'objet d'une décision du Médiateur.

Afin d'éviter les doubles emplois inutiles et d'assurer une approche cohérente des questions liées à la protection des données, tant générales que spécifiques, que soulèvent les plaintes, un mémorandum d'accord a été signé en novembre 2006 entre le Médiateur et le CEPD. Dans la pratique, le mémorandum d'accord a permis, quand cela s'avérait nécessaire, un partage utile d'informations entre le CEPD et le Médiateur. Ce dernier a consulté le CEPD sur des dossiers soulevant des questions relatives à la protection des données et a informé le CEPD de ses décisions concernant des dossiers également soumis au CEPD ou ayant des implications en matière de protection des données. Dans un dossier où l'auteur d'une plainte adressée au CEPD avait également décidé de saisir le Médiateur d'une plainte, les résultats de l'enquête menée par le CEPD ont été transmis au Médiateur afin d'éviter les doubles emplois.

Le CEPD a conseillé le Médiateur sur différentes plaintes liées à l'accès aux documents, conformément aux points C et D du mémorandum d'accord. Il a adressé des observations au Médiateur, qui en a tenu compte dans ses décisions. Ces plaintes ont permis au CEPD de développer sa stratégie

visant à un équilibre entre accès du public aux documents et protection des données et de donner suite à son document de référence de 2005 (disponible sur le site internet du CEPD), dans les cas où l'accès aux informations présente un réel intérêt public. Ces plaintes ont notamment concerné des demandes d'accès de membres du Parlement européen à des régimes de retraite complémentaire, les comptes de tous les membres du Parlement issus d'un État membre et la prorogation du détachement d'un fonctionnaire (au sein de la Commission).

#### 2.4.5. Travaux complémentaires dans le domaine des plaintes

Le CEPD a poursuivi la rédaction d'un manuel interne relatif au traitement des plaintes par les services du CEPD. Les principaux éléments de la procédure, un formulaire type de présentation des plaintes, ainsi que des informations sur la recevabilité des plaintes seront publiés sur le site internet du CEPD le moment venu.

Des membres du personnel ont également participé à Helsinki et à Lisbonne, en avril et en novembre 2007 respectivement, à des ateliers de traitement des dossiers organisés par les autorités nationales compétentes en matière de protection des données. Lors de ces ateliers, le CEPD a présenté des exposés sur l'accès du public aux documents et la protection des données au sein des administrations de l'UE, ainsi que sur les enquêtes internes effectuées par l'OLAF et l'analyse criminologique des ordinateurs.

Le CEPD a également profité de ces ateliers pour partager son expérience et s'informer sur les questions qui se posent actuellement en matière de protection des données au niveau national. Le CEPD a notamment soulevé la question de la mise en œuvre dans les États membres de la directive 2005/60/CE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, qui se pose dans un dossier de contrôle préalable en cours.

## 2.5. Enquêtes

L'article 46, point b), du règlement prévoit que le CEPD peut effectuer des enquêtes, également de sa propre initiative. Le CEPD a mené un certain nombre de ces enquêtes, dont certaines méritent une attention particulière dans le présent rapport (voir également le point 2.9 sur la vidéosurveillance).

### Audit de sécurité de l'OLAF

En 2007, le CEPD a reçu de nombreuses notifications de l'OLAF concernant des traitements de données utilisant la même infrastructure informatique. Ce matériel, qui se trou-

vait initialement dans le centre de données de la Commission européenne, a été transféré sur le site de l'OLAF et est désormais directement géré par le personnel de l'OLAF.

Pour garantir une approche cohérente à l'égard des mesures de sécurité de l'OLAF, le CEPD a décidé de réaliser une inspection de sécurité et a examiné ces mesures horizontalement, plutôt que dans le cadre de chaque notification en vue d'un contrôle préalable. Le fait de procéder à cet examen en liaison avec une inspection de sécurité spécifique a également permis de mieux prendre en considération la dimension de confidentialité que revêtent ces mesures de sécurité.

Cette inspection visait essentiellement à collecter des informations sur les mesures de sécurité et de protection des données en vigueur ou à venir et à les comparer aux exigences en la matière afin d'évaluer leur conformité aux normes juridiques et techniques.

Après avoir fourni des orientations, sous la forme de recommandations, en vue de l'amélioration des systèmes, le CEPD a conclu, d'une manière générale, qu'il était très satisfait des mesures de sécurité qui avaient été mises en œuvre par l'OLAF en ce qui concerne les systèmes et les applications informatiques relevant de sa responsabilité.

L'efficacité de la mise en œuvre de ces mesures de sécurité sera évaluée en 2008 au moyen d'un audit de sécurité approfondi prévu par l'OLAF, auquel le CEPD sera associé en tant qu'observateur.

### SWIFT

Le 1<sup>er</sup> février 2007, le CEPD a rendu son avis sur le rôle de la BCE dans le dossier «SWIFT» (concernant l'accès des autorités américaines aux données bancaires dans le cadre de la lutte contre le terrorisme). Cet avis a mis l'accent sur le rôle de la BCE en tant que superviseur, utilisateur et décideur.

Dans le même temps, dans le cadre de l'action coordonnée menée par les autorités européennes compétentes en matière de protection des données, le CEPD a demandé aux principales institutions communautaires de fournir des éclaircissements sur les systèmes de paiement utilisés et sur les contrats qui les lient à SWIFT.

Le 14 février 2007, le Parlement européen a adopté une résolution commune sur les données des dossiers passagers (données PNR) et sur SWIFT. En ce qui concerne SWIFT, le Parlement a approuvé l'avis rendu par le CEPD et a appelé la BCE et les autres institutions concernées à veiller à ce que les systèmes de paiement européens respectent pleinement le droit européen en matière de protection des données.

Au printemps 2007, à la suite de demandes formulées par le CEPD, la BCE a présenté un rapport sur les mesures qu'elle a prises pour se conformer à l'avis susvisé, et d'autres institutions ont fourni des éclaircissements sur le respect des



MM. Nikiforos Diamandouros, Joaquín Bayo Delgado et Peter Hustinx durant une conférence de presse.

règles en matière de protection des données dans le cadre de leurs systèmes de paiement.

Sur la base des informations reçues, le CEPD a recommandé aux institutions communautaires concernées de prendre des mesures afin de respecter pleinement les obligations légales leur incombant en vertu du règlement (CE) n° 45/2001, et notamment de fournir suffisamment d'informations aux membres de leur personnel et aux autres personnes qui leur sont liées par contrat.

D'une manière plus générale, en tant que membre du groupe de l'article 29, le CEPD a suivi de près les progrès accomplis dans ce dossier:

- l'adhésion de SWIFT aux principes de la «sphère de sécurité» (*Safe Harbor*), qui permet de couvrir les transferts à des fins commerciales vers le centre de traitement des États-Unis;
- les éclaircissements et les assurances fournis par le département du Trésor des États-Unis concernant des aspects essentiels relatifs à l'accès aux données SWIFT et à leur traitement à la suite d'injonctions, comme la finalité, la proportionnalité, le contrôle et les mécanismes de règlement des litiges;
- l'annonce de modifications importantes, à long terme, de l'architecture des services de paiement SWIFT: l'établissement d'un nouveau centre de traitement en Suisse permettra aux messages émis en Europe d'y rester et de ne plus être communiqués aux États-Unis.

En 2008, le CEPD, travaillant en coordination avec d'autres autorités compétentes en matière de protection des données, entend continuer d'encourager et de suivre de près les progrès réalisés dans ce domaine.

## 2.6. Action en matière d'inspection

### 2.6.1. L'échéance du «printemps 2007» et au-delà

Conformément à l'article 41, paragraphe 2, du règlement (CE) n° 45/2001, le CEPD est chargé de surveiller et d'assurer l'application dudit règlement. En mars 2007, le CEPD a lancé une procédure visant à évaluer le respect de ce règlement au sein des différentes institutions et des différents organes et à pérenniser les effets de l'échéance fixée au «printemps 2007» (voir le point 2.3).

La première phase de cette procédure, lancée en 2007, a consisté à adresser des lettres aux directeurs de l'ensemble des institutions et organes pour faire le point des progrès accomplis jusqu'alors dans les différents services de l'administration de l'UE.

Dans cette première phase, le CEPD a adopté une approche progressive, en fonction de la date de création de l'institution ou de l'organe.

Pour une série d'organes, la première étape a consisté à inviter les directeurs à désigner un DPD. En effet, en mars 2007, dix organes opérationnels n'avaient pas encore désigné de DPD. Des copies des différentes lettres envoyées ont été adressées aux DG responsables de la Commission afin de souligner la nécessité de fournir aux DPD les ressources nécessaires à l'exercice de leurs fonctions.

Depuis l'envoi de ces lettres, tous les organes opérationnels ont désigné un DPD, même si le DPD de l'un de ces organes n'a été désigné qu'à titre provisoire. Par ailleurs, en novembre 2007, le CEPD a été informé de la désignation d'un DPD au sein du Fonds européen d'investissement, dont les fonctions avaient jusqu'alors été exercées par le DPD de la Banque européenne d'investissement.

En avril 2007, le CEPD a adressé des lettres aux institutions et organes disposant déjà d'un DPD, les invitant à répondre à quatre séries de questions, concernant:

- 1) le statut du DPD;
- 2) un inventaire des traitements portant notamment sur des données à caractère personnel;
- 3) un inventaire des traitements relevant de l'article 27 du règlement (CE) n° 45/2001;
- 4) la poursuite de la mise en œuvre du règlement.

Une note spécifique a été envoyée au responsable administratif du CEPD, institution elle-même soumise au règlement (CE) n° 45/2001, afin de solliciter des informations sur l'inventaire des traitements, l'inventaire des traitements soumis au contrôle préalable et d'autres mesures de mise en œuvre.

## 2.6.2. Délégués à la protection des données

### Désignation des DPD

Comme indiqué ci-dessus, la totalité des institutions et organes communautaires ont désigné un DPD. Les grandes institutions ont également désigné un DPD adjoint (Parlement européen, Conseil de l'Union européenne, Commission européenne, Cour de justice). Dans la plupart des cas, les DPD adjoints exercent leurs fonctions à temps plein. Certaines institutions ont également désigné des coordinateurs de la protection des données ou des personnes de contact.

### Indépendance des DPD

Dans son document de référence sur les DPD <sup>(19)</sup>, le CEPD a souligné que certains éléments pouvaient compromettre l'indépendance des DPD au sein des institutions/organes, à savoir le fait qu'ils exercent leur fonction à temps partiel (et que, par conséquent, ils sont susceptibles de rencontrer des difficultés pour consacrer le temps prévu à leur mission de DPD) ainsi que leur position hiérarchique et la personne à laquelle ils doivent rendre compte.

Les grandes institutions (Parlement, Conseil et Commission) disposent, quant à elles, d'un DPD exerçant ses fonctions à temps plein. L'OHMI a temporairement désigné un DPD à temps plein pour la période allant de février à décembre 2007 afin qu'il se consacre aux questions à traiter. L'ensemble des autres institutions/organes disposent d'un DPD exerçant ses fonctions à temps partiel, sans que le temps consacré à ses fonctions de DPD soit clairement fixé. Dans la plupart des cas, le DPD est également conseiller juridique.

Le CEPD a par ailleurs souligné que l'indépendance était liée à la position hiérarchique du DPD et à la personne à laquelle il doit rendre compte. La plupart des institutions et organes ont fourni des garanties à cet égard, le DPD étant rattaché au secrétaire général ou à un directeur et le CEPD étant consulté avant l'évaluation du travail du DPD.

### Mise à disposition du personnel et des ressources nécessaires

Le CEPD a souligné que le DPD devait disposer du personnel et des ressources nécessaires pour exercer ses fonctions (dans les domaines informatique, des ressources humaines, de la formation et des ressources financières).

<sup>(19)</sup> Voir «Document de référence sur le rôle joué par les délégués à la protection des données pour garantir le respect effectif du règlement (CE) n° 45/2001» (disponible sur le site internet du CEPD à partir de l'onglet «Consultation»).

La plupart des institutions et organes ont fourni des informations pertinentes concernant les ressources et le personnel mis à la disposition du DPD pour exercer ses fonctions. Dans certains cas, des DPD adjoints ont été désignés. Dans d'autres, le DPD bénéficie de l'assistance d'autres services, par exemple du service juridique.

En ce qui concerne les questions budgétaires, une seule institution a indiqué le budget affecté au DPD. Certaines institutions, toutefois, tiennent à souligner qu'elles n'ont jamais refusé aucun engagement budgétaire.

Certaines institutions et certains organes font mention des formations dont bénéficie le DPD, qui prennent essentiellement la forme d'une participation aux réunions de DPD ou à des formations organisées par le CEPD. Un certain nombre d'institutions/organes ont fait observer qu'ils avaient mis en place un système informatique dédié à la protection de données.

## 2.6.3. Inventaire des traitements

Bien qu'il ne s'agisse pas d'une obligation légale, le CEPD considère que l'inventaire de tous les traitements effectués au sein d'une institution ou d'un organe constitue un moyen utile de vérifier que le règlement est respecté. En conséquence, le CEPD a invité les institutions et organes à établir un tel inventaire et à le lui présenter. Le CEPD a également sollicité des informations concernant l'obligation de notifier les traitements au DPD.

La plupart des institutions et organes ont établi (ou établissent actuellement) cet inventaire, qui leur permet d'évaluer leur niveau de conformité au règlement.

## 2.6.4. Inventaire des dossiers de contrôle préalable

Dans ses lettres, le CEPD a sollicité un aperçu du respect des dispositions en matière de contrôle préalable. Il a demandé que lui soient fournis un inventaire récent de tous les traitements soumis au contrôle préalable, accompagné d'informations sur l'état de ces dossiers, ainsi qu'un point de la situation sur les dossiers relevant des premiers domaines prioritaires (dossiers médicaux, évaluation du personnel, procédures disciplinaires, services sociaux et contrôle des communications électroniques).

La plupart des institutions et organes ont établi cet inventaire, permettant au CEPD de vérifier le respect de l'article 27 du règlement. Le lancement de la procédure concernant l'échéance du «printemps 2007» a entraîné une augmentation considérable des notifications en vue d'un contrôle préalable a posteriori, comme indiqué ci-dessus (voir le point 2.3.4). Dans certains cas, il a même entraîné la notification de tous les cas examinés a posteriori au sein de l'institution. Cette procédure a également été l'occasion

pour les institutions et organes d'informer le CEPD de l'état d'avancement de certains dossiers et traitements en suspens dans des domaines prioritaires.

### 2.6.5. Poursuite de la mise en œuvre

Le CEPD a également demandé aux institutions et organes communautaires de l'informer de la poursuite de la mise en œuvre du règlement, y compris de l'adoption de dispositions d'application, et de sensibiliser le personnel aux questions relatives à la protection des données. Il a demandé aux institutions et organes de lui envoyer un modèle des déclarations relatives au respect de la vie privée qu'ils utilisent et a demandé à être informé des moyens habituels auxquels les personnes concernées peuvent recourir pour exercer leurs droits.

L'article 24, paragraphe 8, du règlement dispose que des dispositions complémentaires d'application sont adoptées par chaque institution ou organe communautaire. Elles concernent en particulier les tâches, les fonctions et les compétences du DPD.

Huit institutions/organes seulement ont adopté des dispositions d'application à ce jour. Quatre institutions/organes prévoient d'en adopter en 2008 et deux organes prévoient de commencer à examiner de telles dispositions. Un certain nombre d'institutions/organes n'ont donc pas encore adopté de dispositions d'application.

À des fins de sensibilisation, des informations relatives à la protection des données sont généralement fournies via les sites intranet et internet concernés, grâce à la publication d'un registre électronique ou dans des brochures ou bulletins d'information. Certaines institutions ont également, de manière active, organisé des formations ou des programmes d'accompagnement destinés aux membres du personnel ou invité des intervenants extérieurs afin de promouvoir la protection des données en leur sein.

Les institutions et organes ont élaboré différentes déclarations relatives au respect de la vie privée, qui fournissent les informations prévues aux articles 11 et 12 du règlement. Les pratiques les plus courantes consistent à publier une déclaration relative au respect de la vie privée sur l'intranet ou l'internet, à fournir des informations dans des notes personnalisées au personnel, à afficher des avis concernant la protection de la vie privée aux endroits de passage les plus fréquentés ou à intégrer des exigences en matière de protection des données dans d'autres documents (contrats par exemple).

Par ailleurs, parmi les moyens auxquels les personnes concernées peuvent recourir pour exercer leurs droits figure généralement la possibilité de contacter le DPD ou le responsable du traitement ou celle d'envoyer un message dans une boîte aux lettres électronique générale à cet effet. Certains

DPD ont également élaboré des formulaires électroniques, disponibles sur l'intranet de leur institution/organe.

### 2.6.6. Conclusions

La procédure dont l'échéance a été fixée au «printemps 2007» a permis au CEPD de faire le bilan du niveau de conformité des institutions et organes avec le règlement (CE) n° 45/2001. Le CEPD a élaboré un rapport général sur la question. La procédure susvisée a obligé les organes qui ne l'avaient pas encore fait à désigner un DPD et à examiner la question des ressources et du personnel nécessaires à l'exercice de ses fonctions. Cette procédure a également encouragé les institutions/organes à identifier les traitements de données à caractère personnel et à déterminer quels traitements devaient être soumis au contrôle préalable du CEPD. Elle a incité les institutions et organes à résorber l'arriéré des dossiers de contrôle préalable a posteriori, ce qui a entraîné une augmentation considérable des dossiers présentés au CEPD en vue d'un contrôle préalable.

La procédure susvisée doit être considérée comme le début d'un exercice permanent du CEPD visant à garantir le respect du règlement, donnant lieu à d'éventuelles vérifications sur place ainsi qu'à des demandes régulières du CEPD aux directeurs des institutions et organes en vue d'évaluer les progrès accomplis en la matière.

## 2.7. Mesures administratives

L'article 28, paragraphe 1, du règlement confère au CEPD le droit d'être informé des mesures administratives relatives au traitement de données à caractère personnel. Le CEPD peut rendre un avis soit à la demande d'une institution ou d'un organe, soit de sa propre initiative. L'article 46, point d), renforce ce mandat pour ce qui est des dispositions d'application du règlement, en particulier celles qui concernent les DPD (article 24, paragraphe 8).

Dans le cadre de consultations menées sur des mesures administratives envisagées par les institutions ou organes communautaires, plusieurs questions délicates ont été soulevées, dont la fixation de périodes de conservation pour certaines catégories de dossiers, les documents stratégiques relatif à l'internet, les procédures d'enquête contre la fraude et la corruption, les échanges d'informations, les dispositions d'application concernant la protection des données et l'applicabilité du droit national en matière de protection des données.

### Périodes de conservation de certaines catégories de dossiers

La Commission européenne a consulté le CEPD sur un projet de liste de conservation commune (LCC). La LCC a

pour objectif de fixer des périodes de conservation des documents avant leur élimination, que les DG/départements appliqueront à certaines catégories de dossiers, compte tenu de leur utilité administrative et des obligations légales.

Le CEPD s'est réjoui que la LCC fasse référence à ses avis sur des notifications en vue d'un contrôle préalable dans les domaines de la sélection, des enquêtes internes, des aides sociales et financières, ainsi que de la période de conservation des dossiers disciplinaires (dossier 2007-222).

Néanmoins, le CEPD a demandé que soient justifiées, en particulier:

- la conservation des dossiers contenant des données administratives et financières sur l'organisation des conférences d'information;
- la conservation des dossiers de mise en œuvre des politiques de ressources humaines pendant une durée de dix ans pour autant que ces dossiers contiennent des données à caractère personnel;
- la conservation des dossiers personnels jusqu'à huit ans après l'extinction de tous les droits de la personne concernée et de ses ayants droit au moins cent vingt ans après la date de naissance cette personne.

### Procédures d'enquête

L'OLAF a présenté au CEPD la version abrégée du manuel révisé de l'OLAF concernant les principes réglementaires et de procédure de l'Office, ses procédures d'enquête ainsi que les droits de la personne et les obligations d'information. Le CEPD a rappelé son avis du 23 juin 2006 concernant une notification relative à un contrôle préalable à propos des enquêtes internes effectuées par l'OLAF (dossier 2005-418). Il a recommandé d'indiquer, dans une prochaine version du manuel de l'OLAF, que la règle générale appliquée consiste à autoriser l'accès aux données à caractère personnel relatives à la personne concernée contenues dans le dossier, sauf si un tel accès devait nuire à l'enquête, une telle exception faisant l'objet d'une décision au cas par cas et n'étant jamais appliquée systématiquement. Le CEPD a demandé à être consulté avant l'adoption de la nouvelle version, plus étoffée, du manuel de l'OLAF (dossier 2007-310).

Le CEPD a rendu un avis sur un projet de décision de la Cour de justice modifiant une décision antérieure concernant les conditions dans lesquelles sont menées les enquêtes internes dans le domaine de la lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts financiers de la Communauté. Le CEPD a rappelé l'avis qu'il a rendu sur les enquêtes internes effectuées par l'OLAF (dossier 2005-418), soulignant que les garanties fournies aux personnes concernées étaient conformes aux orientations qu'il a formulées dans cet avis. Néanmoins, il a recommandé la mention expresse de l'obligation de confidentialité concer-

nant l'identité de l'informateur, ainsi que des articles 11 et 12 du règlement (CE) n° 45/2001 (dossier 2007-167).

### Échange d'informations entre l'OLAF et Eurojust

L'OLAF a présenté au CEPD un projet d'accord concernant des procédures de coopération entre l'OLAF et Eurojust, qui définit essentiellement les modalités d'un échange d'informations entre ces deux organes, y compris de données à caractère personnel, et qui, dans certains cas, souligne ou précise également certains éléments du cadre juridique existant. Outre les quelques suggestions de reformulation qu'il a émises à des fins de clarification, le CEPD a souligné que l'OLAF devrait prévoir le droit pour les personnes concernées d'être informées du transfert de données vers Eurojust ou d'éventuels transferts ultérieurs. Il a indiqué qu'un tel droit pourrait exister en vertu de l'article 11, paragraphe 1, point c), et de l'article 12, paragraphe 1, point c), du règlement (CE) n° 45/2001, à moins qu'une exception ne s'applique (dossier 2007-258).

### Documents stratégiques relatifs à l'internet

Le CEPD a également été consulté par le DPD de la Cour des comptes européenne concernant le document stratégique relatif à l'internet de cette institution. Le CEPD a indiqué que, étant donné, d'une part, que le contrôle de l'utilisation de l'internet décrit dans les orientations en matière de sécurité de l'internet entraînait l'évaluation du comportement des utilisateurs et, d'autre part, qu'un tel contrôle donnait lieu à la collecte de données relatives à des suspicions, ce contrôle était, en principe, susceptible d'être soumis au contrôle préalable en vertu de l'article 27, paragraphe 2, points a) et b), du règlement.

L'une des nombreuses recommandations concrètes du CEPD concerne la fixation d'une période pendant laquelle les fichiers historiques sont conservés à des fins de contrôle et la communication de ce délai aux utilisateurs dans le cadre des orientations en matière de sécurité de l'internet (dossier 2007-593).

Le CEPD a salué l'initiative du DPD du Parlement européen concernant un protocole de bonnes pratiques dans le cadre des enquêtes menées en cas de soupçon d'utilisation abusive de l'accès à l'internet ou d'une messagerie électronique. Le CEPD a indiqué que le contrôle des communications électroniques constituait un nouvel élément dans le cadre des enquêtes menées en cas de soupçon d'utilisation abusive de l'internet ou d'une messagerie électronique et a donc recommandé que ce protocole soit soumis au contrôle préalable du CEPD, en application de l'article 27 du règlement. Le CEPD a notamment fait remarquer que l'abus devait présenter un certain degré de gravité, afin d'éviter des enquêtes inutiles. En outre, à des fins d'information, il a recommandé de faire référence à l'article 20 du règlement (conditions dans

lesquelles l'obligation d'information peut être reportée). Le CEPD a également indiqué qu'il importait de préciser, dans le protocole, la nature des enquêtes menées à la demande de la personne concernée. Par ailleurs, il a souligné que les mêmes garanties en matière de protection des données s'appliquaient aux enquêtes administratives en général (dossier 2007-261).

### **Dispositions d'application en matière de protection des données**

Le CEPD a formulé des observations concernant le projet de dispositions d'application en matière de protection des données au sein de l'Agence communautaire de contrôle des pêches (ACCP). Outre une série de modifications substantielles, le CEPD a salué l'approche adoptée par l'ACCP consistant à ne pas limiter les dispositions d'application au DPD, conformément à l'article 24, paragraphe 8, du règlement, mais à les étendre au rôle des responsables du traitement et aux droits des personnes concernées (dossier 2007-651).

Une décision du directeur exécutif adoptant des dispositions d'application en matière de protection des données au sein de l'Agence européenne pour la sécurité maritime a également été soumise au CEPD. Ce dernier a notamment recommandé que les tâches, les fonctions et les compétences du DPD soient décrites, qu'en particulier le traitement des demandes et des plaintes soit mentionné et qu'il soit fait référence aux articles 11 et 12 du règlement (dossier 2007-395).

Par ailleurs, le DPD de l'EMSA a demandé conseil sur un projet relatif à la diffusion, sur l'intranet, de règles en matière de protection des données. Le CEPD a recommandé de procéder à quelques modifications rédactionnelles dans un souci de cohérence avec le règlement (dossier 2007-397).

### **Publication de la jurisprudence nationale sur le portail externe**

Le CEPD a été consulté sur un projet d'avis du DPD de la Cour de justice concernant la publication de la jurisprudence nationale sur le portail externe, qui soulève des questions relatives aux décisions préjudicielles dans le domaine du droit communautaire.

Le CEPD a fait observer que, avant de publier la jurisprudence nationale sur le portail externe, il importait de déterminer la nécessité de cette opération, à la lumière de l'objectif poursuivi. Le CEPD a recommandé à la Cour de justice de réfléchir à une méthode permettant de rendre anonymes les décisions des tribunaux nationaux, en tenant compte du degré de transparence recherché. Lorsque les données ne sont pas rendues anonymes, il convient de prendre en considération l'article 5, points a) et d), et l'article 12 du règlement (dossier 2007-444).

### **Applicabilité du droit national en matière de protection des données**

Le DPD de la Fondation européenne pour l'amélioration des conditions de vie et de travail (Eurofound) a présenté une demande de consultation concernant la politique de l'Eurofound en matière de protection des données relatives au personnel. La Fondation ayant son siège en Irlande, la question de l'applicabilité du droit irlandais a été soulevée. Le CEPD a souligné que, bien que la jurisprudence prévoie que l'immunité des institutions et organes communautaires n'est pas absolue et que le droit national peut s'appliquer lorsqu'un domaine particulier n'est pas couvert par le droit de l'UE et qu'aucune règle spécifique ne s'applique, la mention du droit national en matière de protection de données n'était pas justifiée. Il a formulé d'autres recommandations, concernant par exemple les périodes de conservation des données médicales, des données relatives à des mesures disciplinaires ou au trafic, ainsi que des données relatives au contrôle du serveur d'échange ou à la gestion de la sécurité ou du trafic (dossier 2007-305).

### **Autres questions**

La mise en place d'un réseau de correspondants chargés de la protection des données au sein du Parlement européen, en tant que mesure relevant de l'organisation interne, a également été soumise à consultation. Le CEPD a salué l'idée du DPD du Parlement, soulignant qu'un tel réseau se révélait très utile au sein de la Commission européenne pour promouvoir et contrôler le traitement des données à caractère personnel et pour aider les responsables du traitement à remplir leur mission (dossier 2007-297).

Le DPD de l'Observatoire européen des drogues et des toxicomanies a, quant à lui, demandé conseil sur des décisions concernant les compensations applicables aux heures de travail prestées et missions effectuées les samedis, dimanches et jours fériés, ou entre 22 heures et 7 heures, et concernant un régime souple en matière de congés. Dans ce cas, des données à caractère personnel ayant été collectées dans le cadre de ces deux procédures, le CEPD a indiqué que le règlement s'appliquait, ces décisions ne soulevant pas, en tant que telles, de problèmes particuliers en matière de protection des données (dossier 2007-725).

## **2.8. Contrôle des communications électroniques**

L'utilisation d'outils de communication électronique au sein des institutions et organes de l'UE génère des données à caractère personnel dont le traitement entraîne l'application des dispositions du règlement (CE) n° 45/2001. Le CEPD élabore actuellement des mesures concernant le traitement

des données générées par l'utilisation des communications électroniques (téléphone, messagerie électronique, téléphone mobile, internet, etc.) au sein des institutions et organes de l'UE. Un projet de document relatif au «contrôle des communications électroniques», portant sur l'utilisation et le contrôle du réseau de communication, a été diffusé aux DPD afin de recueillir leurs observations et leurs réactions.

Ces observations et réactions ont été prises en considération et sont intégrées dans un document final qui tient également compte des évolutions récentes dans ce domaine, telle que la décision de la Cour européenne des droits de l'homme selon laquelle le fait de contrôler la manière dont les membres du personnel utilisent l'internet constitue une violation des droits de l'homme<sup>(20)</sup>. Les modifications apportées à l'article 49 des modalités d'exécution du règlement financier général concernant les informations relatives aux transferts aux fins de l'audit et de la conservation des données seront également prises en compte dans le document final.

Des questions ont également été soulevées à cet égard dans le cadre d'autres activités du CEPD et sont examinées ailleurs dans le présent rapport (voir au point 2.3.4 la partie consacrée au contrôle des communications électroniques et au point 2.7 celle concernant les consultations à propos des documents stratégiques relatif à l'internet).

## 2.9. Vidéosurveillance

En 2007, le CEPD a continué de travailler à l'élaboration de lignes directrices dans le domaine de la vidéosurveillance afin de fournir aux institutions et organes communautaires des conseils pratiques sur le respect des règles en matière de protection des données lors de l'utilisation de systèmes de vidéosurveillance. Après avoir procédé en 2006 à une enquête auprès de différentes institutions et de différents organes communautaires concernant leurs pratiques, le CEPD a également réalisé, au printemps 2007, une enquête internationale auprès des États membres de l'UE, avec l'assistance des autorités nationales compétentes en matière de protection des données. Cette enquête a porté sur les règles en matière de protection des données qui régissent les pratiques de vidéosurveillance dans l'ensemble de l'UE.

Dans le même temps, le CEPD a également acquis davantage d'expérience pratique dans le domaine de la vidéosurveillance «en interne». Il a continué de coopérer avec le Parlement européen pour donner suite à une plainte présentée en 2006 concernant les pratiques du Parlement en matière de vidéosurveillance.

Le CEPD a également répondu à trois demandes de consultation relatives à la vidéosurveillance, qui lui ont été transmises par les DPD de deux institutions. Ces dossiers étaient tous trois liés à l'utilisation de la technologie vidéo à des fins non sécuritaires.

<sup>(20)</sup> Affaire *Copland/Royaume-Uni*, requête 62617/00.

Dans le dossier «info-centres» (2006-490), une institution a installé des caméras de vidéosurveillance dans ses info-centres (lieux où les visiteurs peuvent utiliser des ordinateurs et internet). Les images filmées dans ces info-centres, qui montrent des visiteurs à des postes de travail, ont été diffusées en direct sur le site intranet de l'institution, afin de promouvoir ces info-centres. Il s'agissait également d'aider le personnel d'assistance à surveiller l'espace disponible dans les info-centres. Dans son analyse du caractère proportionné du traitement, le CEPD a conclu que ce traitement était intrusif, en particulier au regard des objectifs recherchés et de l'existence d'autres moyens viables permettant d'atteindre ces mêmes objectifs. En conséquence, le CEPD a recommandé à l'institution d'utiliser d'autres méthodes pour promouvoir ses info-centres et surveiller l'espace disponible.

Une autre demande de consultation, concernant le dossier relatif aux quais de déchargement (2006-510), a porté sur une proposition visant à installer des caméras au niveau des quais de déchargement dans le parking d'une institution, afin de surveiller l'espace disponible pour le chargement et le déchargement. L'équipe chargée de l'approvisionnement aurait eu accès en ligne aux images ainsi filmées. Dans ce dossier aussi, le CEPD a recommandé i) d'utiliser d'autres méthodes pour surveiller l'espace disponible ou bien ii) de positionner les caméras ou de définir leur résolution de telle sorte qu'aucune personne filmée ne soit identifiable.

Un troisième dossier (concernant des installations vidéo dans des salles de conférence — dossier 2007-132) a mis l'accent sur la manière dont il convient d'informer les intervenants et/ou les participants, et d'obtenir leur consentement, lorsqu'ils sont filmés lors d'une conférence ou d'un autre événement particulier tenu dans les locaux de l'institution concernée.

En 2007, le CEPD a également reçu un certain nombre de notifications en vue d'un contrôle préalable émanant d'institutions et d'organes communautaires. Hormis le dossier relatif aux pratiques de l'OLAF dans le cadre de son projet de télévision en circuit fermé (CCTV), toutes les autres notifications en vue d'un contrôle préalable ont concerné des dossiers examinés a posteriori.

La Commission, le CCR à Ispira, le Conseil ainsi que le Comité des régions, conjointement avec le Comité économique et social européen, ont présenté chacun au CEPD une notification, dans le domaine de la vidéosurveillance, en vue d'un contrôle préalable a posteriori. Ces dossiers ont été suspendus, en attendant l'adoption des lignes directrices du CEPD dans le domaine de la vidéosurveillance. Toutefois, les pratiques de l'OLAF dans le cadre de son projet de CCTV, faisant l'objet d'une véritable procédure de contrôle préalable, sont actuellement examinées par le CEPD (dossier 2007-634).

Sur la base des résultats des deux enquêtes menées, et de l'expérience acquise jusqu'alors, le CEPD a commencé à élaborer à la fin de 2007 son premier projet de lignes direc-

trices dans le domaine de la vidéosurveillance, qui sera soumis à consultation. Il est prévu que ce projet sera achevé et publié sur le site internet du CEPD en 2008 et que toutes les parties intéressées seront invitées à formuler des observations y afférentes. Le CEPD prévoit d'adopter la version finale de ses lignes directrices après avoir examiné les observations reçues et, au vu de celles-ci, avoir procédé aux éclaircissements et améliorations appropriés. Ces lignes directrices mettront l'accent sur des questions relatives aux pratiques des institutions et organes de l'UE, mais s'inspireront également des législations nationales en matière de protection des données, ainsi que des réglementations et lignes directrices existant dans les États membres de l'UE.

Elles fourniront des conseils clairs et précis aux institutions ou organes de petite taille, disposant de systèmes de vidéosurveillance relativement simples et peu intrusifs dans la vie privée, et, dans de nombreux cas, limiteront ainsi le nombre de traitements que les responsables du traitement devront soumettre au CEPD en vue d'un contrôle préalable.

Néanmoins, certains systèmes plus complexes, récents ou intrusifs, en particulier les systèmes de vidéosurveillance dits de pointe, resteront soumis au contrôle préalable du CEPD. Ils ne seront approuvés qu'au cas par cas. Les systèmes pour lesquels le responsable du traitement, en raison d'éléments particuliers du dossier, souhaite s'écarter de l'une ou de plusieurs recommandations générales formulées par le CEPD dans ses lignes directrices, dans le domaine de la vidéosurveillance, devront également être soumis au contrôle préalable, prenant dans certains cas une forme simplifiée.

## 2.10. Eurodac

Eurodac est une vaste base de données regroupant les empreintes digitales des demandeurs d'asile et des immigrants clandestins se trouvant sur le territoire de l'UE. Cette base de données contribue à l'application effective de la convention de Dublin en ce qui concerne le traitement des demandes d'asile. Eurodac a été établi en vertu de règles spécifiques au niveau européen, y compris de garanties en matière de protection des données <sup>(21)</sup>.

Le CEPD contrôle le traitement des données à caractère personnel contenues dans la base de données centrale, gérée par une unité centrale au sein de la Commission européenne, ainsi que leur transmission aux États membres. Les autorités chargées de la protection des données dans les États membres contrôlent les traitements de données effectués par les autorités nationales, ainsi que la transmission de ces données à l'unité centrale. Afin de garantir une approche coordonnée, le CEPD et les autorités nationales se réunissent régulièrement pour examiner des problèmes communs liés au fonc-

<sup>(21)</sup> Règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, JO L 316 du 15.12.2000, p. 1.



La surveillance des communications électroniques doit respecter les principes de la protection des données.

tionnement d'Eurodac et pour recommander des solutions communes. Cette approche de «contrôle coordonné» s'est révélée très efficace jusqu'à présent (voir le point 4.3).

En 2005, le CEPD a effectué une inspection afin d'examiner les mesures de sécurité et de protection des données au sein de l'unité centrale. Dans son rapport, publié en février 2006, le CEPD a formulé un ensemble de recommandations visant à améliorer le système.

Dans un deuxième temps, un audit de sécurité approfondi a été lancé, en septembre 2006. Il a permis d'évaluer la conformité des mesures de sécurité mises en œuvre avec les exigences découlant des règles applicables et de la stratégie correspondante de la Commission européenne en matière de sécurité. Il a également permis de déterminer dans quelle mesure ces dispositions de sécurité respectaient encore les bonnes pratiques actuelles. Le rapport d'audit final a été présenté en novembre 2007.

Conformément à un accord entre le CEPD et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), cette dernière a établi des contacts avec des organisations nationales d'experts et a fourni des conseils sur la méthode relative à l'audit de sécurité. L'équipe d'audit était composée de représentants du CEPD, de l'Office fédéral pour la sécurité en matière de technologies de l'information (BSI, Allemagne) et de la direction centrale de la sécurité des systèmes d'information (DCSSI, France). L'ENISA a vérifié la qualité du rapport élaboré. Ce rapport est «Restreint UE», mais un bref résumé a été publié sur le site internet du CEPD <sup>(22)</sup>.

Le CEPD a analysé les conclusions et les recommandations présentées. La principale conclusion était que les mesures de

<sup>(22)</sup> Voir l'onglet «Supervision», rubrique «Eurodac».

sécurité initialement mises en œuvre en ce qui concerne Eurodac et leur maintien au cours des quatre premières années d'activité avaient jusqu'alors fourni un niveau correct de protection. Néanmoins, certaines parties des systèmes, ainsi que la sécurité organisationnelle, présentent des faiblesses qu'il conviendra de pallier afin qu'Eurodac satisfasse pleinement aux bonnes pratiques et applique les meilleures techniques disponibles.

Le CEPD examinera la mise en œuvre des mesures de suivi qui seront élaborées sur la base de ce rapport. Il espère que ledit rapport sera également pris en compte dans le VIS, le SIS II et d'autres systèmes futurs à grande échelle de l'UE.



**Des systèmes de protection des données sont nécessaires pour garantir une utilisation sûre de la vidéosurveillance.**

## 3. Consultation

### 3.1. Introduction

En 2007, le CEPD a continué d'exercer sa fonction de conseiller à l'égard de propositions législatives communautaires et autres documents connexes. Cette fonction est décrite formellement à l'article 28, paragraphe 2, et à l'article 41 du règlement (CE) n° 45/2001.

Comme lors des années précédentes, les activités consultatives du CEPD ont été centrées essentiellement sur l'incidence des propositions législatives relevant de différents domaines d'activité en liaison avec la protection des données. Ce rôle consultatif est garanti par le cadre juridique général concernant la protection des données établi en vertu du traité CE (principalement la directive 95/46/CE relative à la protection des données), ainsi que conformément aux principes généraux de la protection des données applicables en vertu du titre VI du traité UE (le «troisième pilier», domaine d'intervention important pour le CEPD).

Cependant, plus qu'au cours des années précédentes, l'avenir du cadre juridique concernant la protection des données a lui-même compté parmi les activités du CEPD. Premièrement, le CEPD a accordé une grande attention à la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale<sup>(23)</sup>. Deuxièmement, dans son avis<sup>(24)</sup> sur la communication de la Commission relative à la mise en application de la directive sur la protection des données<sup>(25)</sup>, il a estimé que, à long terme, des modifications devraient inévitablement être apportées à la directive et qu'il convenait d'y réfléchir au plus tôt. Troisièmement, le traité de Lisbonne a des conséquences considérables pour la protection des données. Avant la mise au point du traité, le CEPD a attiré l'attention de la présidence portugaise sur quelques points particuliers.

<sup>(23)</sup> COM(2005) 475 final.

<sup>(24)</sup> Avis du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255 du 27.10.2007, p. 1.

<sup>(25)</sup> Communication de la Commission au Parlement européen et au Conseil du 7 mars 2007 intitulée «Suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données» [COM(2007) 87 final].

En outre, le CEPD a examiné pour la première fois la nécessité de disposer d'un cadre juridique spécifique pour la protection des données dans un domaine particulier (l'utilisation de la technologie RFID) dans le cas où le cadre juridique général existant ne serait pas appliqué de manière appropriée. Ce domaine particulier, qui est essentiellement nouveau, peut exercer une incidence importante sur notre société et sur la protection des droits fondamentaux, tels que la protection de la vie privée et des données à caractère personnel.

Deux autres points doivent être soulignés en ce qui concerne l'année 2007:

- Pour la première fois, le CEPD s'est prononcé contre l'adoption d'un instrument juridique proposé par la Commission; cette conclusion figure dans son avis sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives<sup>(26)</sup>.
- Pour la première fois et en deux occasions, le CEPD s'est prononcé sur une communication de la Commission (voir le point 3.3.2).

Les activités du CEPD ont eu lieu dans le contexte de différentes évolutions ayant pour dénominateur commun le fait qu'elles contribuent toutes à l'émergence d'une «société de la surveillance». Elles sont décrites ci-après.

- Dans le domaine de la liberté, de la sécurité et de la justice, les grandes tendances se poursuivent. De nouveaux instruments ont été proposés pour élargir les possibilités de collecte, de conservation et d'échange de données à caractère personnel par les services répressifs, en particulier aux fins de lutte contre le terrorisme et la criminalité organisée.
- Les répercussions de la technologie sur la protection de la vie privée et des données à caractère personnel deviennent de plus en plus visibles. L'utilisation accrue de la biométrie et le développement de la technologie RFID requièrent une attention spécifique.
- L'importance croissante des flux internationaux de données engendre des difficultés de traçabilité. En tout état de cause, ils ne sont pas entièrement couverts par la

<sup>(26)</sup> Avis du 20 décembre 2007.



Une partie de l'équipe de consultation discute d'un avis dans le domaine législatif.

législation de l'UE relative à la protection des données, qui a un champ d'application territorial limité.

En ce qui concerne les méthodes de travail du CEPD, 2007 a été la première année pour laquelle les priorités d'action du CEPD ont été énoncées dans un document public — l'inventaire 2007 — qui a été publié sur le site internet du CEPD en décembre 2006.

Le nombre d'avis rendus a connu la plus petite augmentation possible par rapport à 2006: 12 avis ont été rendus en 2007 contre 11 en 2006. Le CEPD a recouru davantage à d'autres instruments d'intervention, tels que les observations (qui sont également publiées sur le site internet, mais pas au *Journal officiel de l'Union européenne*). Il ne faut pas voir dans le choix de cet instrument un changement structurel d'approche.

Enfin, dans le présent chapitre seront examinées non seulement les activités exercées tout au long de 2007, mais également les nouvelles évolutions technologiques et législatives.

### 3.2. Cadre d'action et priorités

On peut considérer que le document stratégique intitulé *Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes* <sup>(27)</sup> fixe les grandes lignes suivies par le CEPD dans le domaine de la consultation.

Ce document comprend trois éléments: la portée de la mission consultative, la teneur des avis et, enfin, la ligne de conduite et les méthodes de travail. Il a été publié en mars 2005 et s'est révélé être une base solide pour les activités du CEPD.

<sup>(27)</sup> Disponible sur le site internet du CEPD à la rubrique «Consultation».

Cette base a été développée et précisée en 2007. Le CEPD a précisé que l'objectif de sa participation au processus législatif de l'UE est de veiller activement à ce que les mesures législatives ne soient adoptées qu'après un examen approfondi de leur incidence sur la protection de la vie privée et des données à caractère personnel. Les analyses d'impact réalisées par la Commission doivent accorder l'attention voulue à cet aspect. En outre, les décisions doivent toujours être fondées sur la connaissance de leur incidence sur la protection des données.

Par ailleurs, un documentaliste du service du CEPD a entrepris d'établir un rapport sur les lignes et les principes communs mis au point par

le CEPD dans le cadre de ses activités de consultation concernant l'espace de liberté, de sécurité et de justice. Il convient de considérer ce rapport comme un nouveau progrès dans la promotion d'une approche cohérente et comme un facteur essentiel d'efficacité. À ce stade, le CEPD a choisi un champ d'application relativement limité — l'espace de liberté, de sécurité et de justice — mais, à plus long terme, une initiative similaire pourrait être envisagée pour l'ensemble de son domaine d'activité. Le rapport sera terminé au début de 2008.

En ce qui concerne l'approche et les méthodes de travail, 2007 s'est révélée être une année de consolidation. La consultation du CEPD — qui comprend les activités menées aux différentes étapes de la procédure législative — est devenue une partie normale de cette procédure, pour autant naturellement que les propositions aient ou soient susceptibles d'avoir des répercussions sur la protection des données.

#### L'inventaire

L'inventaire annuel doit être vu comme une partie additionnelle du cadre d'action du CEPD. Il est constitué de deux parties:

- une introduction présentant une analyse succincte du contexte et spécifiant les priorités pour l'année considérée;
- une annexe énumérant les propositions de la Commission (et les documents connexes) pour lesquelles une réaction du CEPD est susceptible d'être requise; la principale source de l'annexe est le programme législatif et de travail de la Commission.

L'inventaire 2007 énumère huit priorités pour le CEPD. De manière générale, ce dernier les a respectées. Un examen plus attentif des différentes priorités permet de tirer les conclusions figurant ci-après.

L'annexe de l'inventaire 2007 cite 16 documents importants (qualifiés de «rouges») sur lesquels le CEPD a l'intention de rendre un avis. Les résultats obtenus sont les suivants:

Avis rendu	8 documents
Aucun avis du CEPD, mais soutien à l'avis du WP 29	1 document (accord sur les données PNR avec les États-Unis)
Avis du CEPD reportés à 2008	2 documents
Proposition de la Commission reportée à 2008	5 documents

En outre, la liste contient 22 documents de moindre importance soumis au CEPD, au sujet desquels celui-ci avait l'intention de rendre éventuellement un avis, de réagir d'une autre manière ou tout simplement de suivre de près les évolutions dans ce domaine.

L'état des travaux à la fin de 2007 offre une image diversifiée.

Attention continue du CEPD (programmes de recherche, questions/matières générales, telles que l'immigration ou la santé publique)	8 documents
Intervention du CEPD en 2007 (observations ou action informelle)	4 documents (spams, cybercriminalité, terrorisme, partenariat public-privé)
Supprimé de la liste sans autre intervention du CEPD	5 documents
Activité de la Commission reportée à 2008	2 documents
Transformé en question «rouge» dans l'inventaire 2008	3 documents

## Inventaire 2008

L'inventaire 2008 (le second inventaire annuel) a été publié sur le site internet en décembre 2007. Il s'inscrit, dans les grandes lignes, dans le prolongement de l'inventaire 2007. Les priorités sont présentées d'une manière légèrement différente: l'inventaire 2008 n'énumère que **six priorités**, dont deux sont nouvelles. En 2008, priorité sera également donnée à la préparation de l'entrée en vigueur du traité de Lisbonne, ainsi qu'aux aspects extérieurs de la protection des données liés au transfert de données à des pays tiers.

Dans l'annexe de l'inventaire, on peut voir que le champ d'activité du CEPD couvre à présent un large éventail de domaines d'action. Les propositions citées concernent 13 services différents de la Commission (DG Personnel et administration, DG Emploi, affaires sociales et égalité des chances, DG Entreprises et industrie, Eurostat, DG Société de l'information et médias, DG Justice, liberté et sécurité, DG Marché intérieur et services, OLAF, DG Relations extérieures, DG Santé et consommateurs, secrétariat général,

**Priorité n° 1:** le stockage et l'échange d'informations dans le cadre de l'espace de liberté, de sécurité et de justice ont représenté, une fois de plus, une activité essentielle du CEPD en 2007 (et ce sera le cas tant que le législateur européen continuera d'accorder la priorité à l'adoption de nouveaux actes législatifs ou à la modification d'actes existants dans ce domaine).

**Priorité n° 2:** la communication de la Commission sur l'avenir de la directive 95/46/CE a donné lieu à un avis détaillé du CEPD, dans lequel celui-ci a appelé encore à de nouvelles modifications.

**Priorité n° 3:** les évolutions dans la société de l'information ont été examinées de près et commentées par le CEPD. Il a notamment été question de l'identification par radiofréquence; le CEPD a été associé à la modification de la directive 2002/58/CE (un avis suivra au début de 2008).

**Priorité n° 4:** pour ce qui est d'inclure la santé publique dans le champ d'action prioritaire du CEPD, les progrès ont été modestes, principalement parce qu'aucune proposition législative dans ce domaine n'a été adoptée en 2007. Cette priorité sera donc maintenue en 2008.

**Priorité n° 5:** de nombreuses activités ont été déployées en rapport avec le travail de l'OLAF. Une attention particulière a été accordée aux échanges de données à caractère personnel avec Europol (cette question a été examinée dans l'avis du CEPD sur la décision Europol) ainsi qu'aux échanges de données avec des pays tiers. Il y a un lien évident avec la supervision, par le CEPD, des traitements de données par l'OLAF.

**Priorité n° 6:** en ce qui concerne la transparence, les activités consultatives ont été postposées dans l'attente de l'arrêt du Tribunal de première instance dans l'affaire Bavarian Lager (arrêt rendu le 8 novembre 2007). Une proposition de modification du règlement (CE) n° 1049/2001 est à présent prévue pour le printemps 2008.

**Priorités n° 7 et n° 8:** thèmes horizontaux et autres activités (en rapport avec les méthodes de travail): les travaux ont bien progressé.

DG Fiscalité et union douanière et DG Énergie et transports).

Le nombre total de propositions citées dans l'annexe est lui aussi en augmentation. L'annexe mentionne à présent 67 dossiers, répartis comme suit:

- 34 dossiers sont classés «rouges», ce qui signifie qu'ils revêtent un caractère hautement prioritaire; 33 dossiers sont classés «jaunes»: il s'agit de documents de moindre importance pour le CEPD, sur lesquels il envisage la possibilité de réagir;
- 29 dossiers portent sur des propositions législatives au sens strict (règlements, directives, décisions et décisions-cadres); les 38 autres dossiers sont des documents non législatifs; il s'agit de communications de la Commission, de recommandations, de programmes de travail ainsi que de documents relatifs à des accords entre l'UE et des pays tiers.

Cette augmentation du nombre de propositions citées dans l'annexe s'explique en partie par le fait que l'annexe est basée sur le programme législatif et de travail de la Commission, qui énumère séparément des dossiers étroitement liés. Le fait que 34 dossiers aient été classés «rouges» ne signifie pas nécessairement que le nombre d'avis rendus par le CEPD augmentera en conséquence.

### 3.3. Avis législatifs

#### 3.3.1. Observations d'ordre général

##### Avis sur les questions relevant du troisième pilier

Le CEPD a rendu douze avis législatifs en 2007. Comme les années précédentes, une partie non négligeable de ces avis porte sur l'espace de liberté, de sécurité et de justice. Cependant, ce domaine représente aujourd'hui un peu moins de 50 % des avis législatifs (cinq sur douze). Ces cinq avis concernent des documents dans le domaine de la coopération policière et judiciaire en matière pénale (le troisième pilier) et comprennent des évolutions fondamentales, notamment du point de vue de la protection des données. C'est le cas du troisième avis sur la proposition de la décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Les autres avis portent sur la proposition de décision portant création d'Europol, les deux initiatives sur la coopération transfrontière (transposant le traité de Prüm et l'accord sur son exécution au niveau de l'UE) et la proposition relative au système PNR européen.

Dans le troisième pilier, l'adoption de nouvelles propositions facilitant le stockage et l'échange d'informations par les services répressifs sans qu'un examen approfondi de l'efficacité des instruments juridiques existants ait été réalisé a constitué

une préoccupation majeure. De nouveaux instruments sont conçus avant que les instruments existants ne soient mis en œuvre correctement. Ce problème s'est posé plus particulièrement en ce qui concerne la transposition du traité de Prüm au niveau de l'UE et le système PNR européen.

Un autre problème, qui a occupé une place centrale dans les avis rendus par le CEPD sur les questions relevant du troisième pilier, a été l'absence d'un cadre juridique complet pour la protection des données. La plupart des propositions comprennent des dispositions spécifiques sur la protection des données visant à établir un cadre général. Néanmoins, aucun cadre juridique satisfaisant n'a encore été mis en place.

Un troisième problème qui se pose est le fait que l'UE impose aux États membres de créer des autorités nationales pour certaines tâches, tout en les laissant libres de décider des conditions de leur fonctionnement, ce qui entrave l'échange d'informations entre États membres et nuit à la sécurité juridique de la personne concernée dont les données sont transférées entre les autorités de différents États membres.

L'échange d'informations avec des pays tiers à des fins répressives est une question distincte, que le CEPD a traitée dans d'autres avis. Il a été préoccupé par l'absence d'harmonisation, ainsi que par le manque de garanties entourant le traitement, par les pays tiers, des données à caractère personnel qui leur ont été transférées.

##### Avis sur des communications

Le CEPD a rendu deux avis à propos de communications importantes de la Commission concernant le futur cadre pour la protection des données. Dans son avis relatif à la mise en application de la directive sur la protection des données <sup>(28)</sup>, le CEPD recense cinq aspects d'un contexte en mutation, l'un étant l'interaction avec la technologie. Les nouvelles évolutions technologiques ont des répercussions évidentes sur les exigences liées à un cadre juridique efficace régissant la protection des données. Parmi ces évolutions, l'identification par radiofréquence revêt une importance particulière et fait l'objet d'un avis distinct du CEPD <sup>(29)</sup>.

Les deux avis qu'il a rendus sur les communications de la Commission ont donné au CEPD l'occasion de réfléchir aux perspectives futures de la protection des données et de relancer les discussions sur le cadre de la protection des données dans un avenir proche; ces discussions sont nécessaires et deviennent urgentes (voir le point 3.7 sur les évolutions futures).

<sup>(28)</sup> Avis du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255 du 27.10.2007, p. 1.

<sup>(29)</sup> Avis du 20 décembre 2007 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique» [COM(2007) 96].

### Avis sur la législation relevant du premier pilier

Les cinq autres avis rendus en 2007 par le CEPD sont de diverses natures et portent sur des domaines d'action tels que les douanes, les statistiques, le transport routier, l'agriculture et la sécurité sociale. Le principal dénominateur commun est que trois de ces cinq avis concernent des propositions facilitant l'échange de données entre les autorités des États membres (dans les domaines des douanes, du transport routier et de la sécurité sociale). Parmi les autres questions couvertes figurent la publication d'informations sur les bénéficiaires des fonds communautaires, la notion de confidentialité statistique et le lien entre les règles spécifiques et le cadre général régissant la protection des données.

Les propositions traduisent une tendance plus générale. L'échange d'informations entre les États membres — y compris l'échange de données à caractère personnel — est considéré comme un important instrument du développement du marché intérieur. Faciliter cet échange par le biais de l'utilisation de toutes les possibilités offertes par les réseaux électroniques permettrait de supprimer des obstacles. Parfois, la Commission se voit confier le rôle de responsable de la maintenance et de la disponibilité de l'infrastructure technique. Dans ces cas, le CEPD sert également d'autorité de contrôle.

De manière générale, cette tendance requiert une attention particulière de la part du CEPD, qui doit veiller à ce que les instruments facilitant l'échange de données à caractère personnel comportent des protections et des garanties pour les personnes concernées. À cet égard, il est également essentiel que les personnes concernées puissent exercer leurs droits de façon simple et pratique.

### 3.3.2. Les avis du CEPD

#### Office européen de police

Europol a été créé en 1995 par une convention conclue entre les États membres. Cette convention présente un désavantage en termes de souplesse et d'efficacité, car toutes les modifications doivent être ratifiées par l'ensemble des États membres, ce qui peut prendre des années, comme l'ont montré des expériences antérieures.

L'objectif principal de la proposition de décision du Conseil remplaçant la convention <sup>(30)</sup>, sur laquelle le CEPD a rendu un avis le 16 février 2007 <sup>(31)</sup>, n'est pas de modifier en profondeur le mandat ou les activités d'Europol, mais de le doter d'une nouvelle base juridique plus souple. La proposition prévoit également des modifications substantielles visant à améliorer encore le fonctionnement d'Europol. Elle étend

<sup>(30)</sup> Proposition de décision du Conseil du 20 décembre 2006 portant création de l'Office européen de police (Europol) [COM(2006) 817 final].

<sup>(31)</sup> Avis du 16 février 2007 sur la proposition de décision du Conseil portant création de l'Office européen de police (Europol) [COM(2006) 817 final], JO C 255 du 27.10.2007, p. 13.

son mandat et établit plusieurs nouvelles dispositions visant à faciliter davantage son travail, par exemple en ce qui concerne l'échange de données entre Europol et d'autres organes de la Communauté européenne ou de l'Union européenne, tels que l'OLAF. La proposition contient également des règles spécifiques relatives à la protection et à la sécurité des données destinées à compléter le cadre juridique régissant la protection des données dans le troisième pilier, qui n'a pas encore été adopté.

Le CEPD conclut dans son avis que la décision du Conseil ne devrait pas être adoptée avant l'adoption d'un cadre relatif à la protection des données garantissant un niveau approprié de protection des données.

Il suggère en outre des améliorations, par exemple:

- veiller à ce que les données collectées lors d'activités commerciales soient exactes;
- appliquer des conditions et des garanties strictes en cas d'interconnexion de bases de données;
- harmoniser les règles relatives aux droits d'accès de la personne concernée, en limitant les exceptions à ces règles;
- inclure des garanties relatives à l'indépendance du délégué à la protection des données d'Europol (qui s'assure au niveau interne de la licéité des traitements de données à caractère personnel);
- soumettre les traitements de données concernant le personnel d'Europol au contrôle du CEPD.

#### Application correcte des réglementations douanière et agricole

Le 22 février 2007, le CEPD a rendu un avis sur une proposition de règlement de la Commission qui prévoit la création ou la mise à jour de divers systèmes informatiques contenant des données à caractère personnel. La proposition vise à renforcer la coopération entre les États membres et la Commission afin d'éviter les violations des réglementations douanière et agricole <sup>(32)</sup>. Les systèmes informatiques comprennent le répertoire européen de données, le système d'information douanier (SID) et le fichier d'identification des dossiers d'enquêtes douanières (FIDE).

Dans son avis <sup>(33)</sup>, le CEPD suggère d'apporter plusieurs modifications à la proposition en vue d'assurer sa compatibilité générale avec le cadre juridique existant sur la protec-

<sup>(32)</sup> Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 515/97 du Conseil relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole [COM(2006) 866 final].

<sup>(33)</sup> Avis du 22 février 2007 sur la proposition de règlement modifiant le règlement (CE) n° 515/97 du Conseil relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole [COM(2006) 866 final], JO C 94 du 28.4.2007, p. 3.

tion des données, ainsi qu'une protection efficace des données à caractère personnel. Il propose, entre autres, les mesures suivantes:

- la Commission devrait procéder à une évaluation appropriée de la nécessité de créer le répertoire européen de données;
- si le répertoire européen de données est créé, le règlement devrait prévoir l'adoption de règles administratives complémentaires déterminant les mesures spécifiques à prendre pour assurer la confidentialité des informations;
- différentes dispositions devraient être modifiées afin de reconnaître le rôle de contrôle du CEPD en ce qui concerne le SID et le FIDE;
- il conviendrait d'adopter, pour ce qui est du contrôle du SID, une approche coordonnée associant les autorités nationales et le CEPD.

### Coordination des systèmes de sécurité sociale

Le 6 mars 2007, le CEPD a rendu un avis sur une proposition de la Commission fixant les modalités d'application du règlement portant sur la coordination des systèmes de sécurité sociale. La proposition couvre toute une série de branches de la sécurité sociale (pensions, prestations de maternité, invalidité, chômage, etc.)<sup>(34)</sup>. Elle vise à moderniser et à simplifier les règles existantes en renforçant la coopération et en améliorant les méthodes d'échange de données entre les institutions de sécurité sociale des différents États membres.

Le CEPD accueille favorablement cette proposition dans la mesure où elle a pour objectif de favoriser la libre circulation des citoyens et d'améliorer le niveau de vie et les conditions d'emploi des personnes qui se déplacent à l'intérieur de l'Union<sup>(35)</sup>. S'il est vrai que la sécurité sociale ne pourrait exister sans échanges de différents types de données à caractère personnel, il est tout aussi vrai qu'un niveau élevé de protection de ces données est nécessaire. Dès lors, le CEPD a recommandé:

- d'accorder la plus grande attention aux principes de base de la protection des données, tels que la limitation de la finalité, ainsi que la proportionnalité en matière de données traitées, d'entités compétentes et de périodes de conservation;
- de veiller à ce que chaque mécanisme proposé pour la conservation et la transmission de données à caractère personnel soit clairement fondé sur des motifs juridiques précis;

<sup>(34)</sup> Proposition de règlement du Parlement européen et du Conseil fixant les modalités d'application du règlement (CE) n° 883/2004 portant sur la coordination des systèmes de sécurité sociale [COM(2006) 16 final].

<sup>(35)</sup> Avis du 6 mars 2007 concernant la proposition de règlement fixant les modalités d'application du règlement (CE) n° 883/2004 portant sur la coordination des systèmes de sécurité sociale [COM(2006) 16 final], JO C 91 du 26.4.2007, p. 15.

- de fournir aux personnes concernées des informations pertinentes sur le traitement de leurs données à caractère personnel;
- de permettre aux personnes concernées d'exercer effectivement leurs droits dans un contexte transfrontière.

### Coopération transfrontière (traité de Prüm)

Le 4 avril 2007, le CEPD a rendu un avis sur l'initiative de quinze États membres visant à rendre le traité de Prüm applicable dans l'ensemble de l'UE, bien qu'il n'ait pas été consulté à ce sujet<sup>(36)</sup>.

L'initiative a pour objectif de renforcer la coopération transfrontière, en particulier aux fins de lutte contre le terrorisme et la criminalité transfrontière. Elle porte sur l'échange de données biométriques (ADN et empreintes digitales) et impose aux États membres de mettre en place des bases de données ADN<sup>(37)</sup>.

Bien que la protection des données joue un rôle important dans cette initiative, les dispositions en la matière sont spécifiques et destinées à venir s'ajouter à un cadre général relatif à la protection des données, qui n'a pas encore été adopté. Un tel cadre est nécessaire pour garantir une protection suffisante aux citoyens, car la décision envisagée rendra beaucoup plus facile l'échange de données relatives à l'ADN et aux empreintes digitales.

Étant donné que le traité de Prüm est déjà entré en vigueur dans certains États membres, les suggestions du CEPD visent principalement à améliorer le texte, sans modifier le système d'échange d'informations proprement dit. Il formule en particulier les observations suivantes:

- l'approche adoptée à l'égard des différents types de données à caractère personnel est bonne: plus les données sont sensibles, plus les fins pour lesquelles elles peuvent être utilisées, ainsi que leur accès, doivent être limitées;
- le Conseil devrait inclure une analyse d'impact et une clause d'évaluation dans la procédure d'adoption; le CEPD a attiré l'attention sur le fait qu'un système élaboré pour un petit nombre d'États membres menant une coopération étroite ne convient pas nécessairement pour une application à l'échelle de l'UE;
- l'initiative ne précise pas la catégorie de personnes dont les données figureront dans la base de données ADN et ne limite pas la période de conservation.

### Financement de la politique agricole commune

La proposition analysée a pour objet de satisfaire à l'obligation de publier des informations sur les bénéficiaires des

<sup>(36)</sup> Avis du 4 avril 2007 sur l'initiative de quinze États membres en vue de l'adoption de la décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, JO C 169 du 21.7.2007, p. 2.

<sup>(37)</sup> Initiative de Prüm, JO C 71 du 28.3.2007, p. 35.



La décision «Prüm» repose sur l'utilisation du matériel ADN.

fonds communautaires. Aux fins de la mise en œuvre de l'initiative européenne en matière de transparence, le règlement (CE, Euratom) n° 1995/2006 du Conseil du 13 décembre 2006<sup>(38)</sup>, sur lequel le CEPD a également rendu un avis, a inséré cette obligation dans le règlement financier.

Le principal aspect examiné par le CEPD dans son avis du 10 avril 2007 porte sur le fait que les États membres devraient assurer la publication annuelle ex post de la liste des bénéficiaires, ainsi que des montants reçus par chaque bénéficiaire au titre des fonds européens, qui relèvent du budget des Communautés européennes.

Dans son avis, le CEPD se déclare favorable à l'intégration du principe de transparence et souligne qu'il convient d'adopter une approche proactive en ce qui concerne les droits des personnes concernées. Cette approche pourrait consister à informer les personnes concernées à l'avance, au moment où leurs données à caractère personnel sont collectées, que ces données peuvent être rendues publiques et à garantir le respect du droit d'accès et du droit d'objection de la personne concernée.

Le CEPD propose, en outre, d'introduire une disposition spécifique qui permettrait de se conformer à l'article 12 du règlement (CE) n° 45/2001. L'objectif poursuivi est d'informer la personne concernée de ce que ses données à caractère personnel sont traitées par les institutions et organes compétents en matière d'audit et d'enquête.

### Protection des données dans le troisième pilier (troisième avis du CEPD)

Le 20 avril 2007, la présidence allemande a consulté le Parlement européen au sujet d'une proposition révisée de déci-

<sup>(38)</sup> Règlement (CE, Euratom) n° 1995/2006 du Conseil du 13 décembre 2006 modifiant le règlement (CE, Euratom) n° 1605/2002 portant règlement financier applicable au budget général des Communautés européennes, JO L 390 du 30.12.2006, p. 1.

sion-cadre du Conseil<sup>(39)</sup>. Cette révision avait pour objectif d'accélérer les négociations au sein du Conseil et d'améliorer la protection des données dans le troisième pilier. Le CEPD a estimé que les modifications substantielles figurant dans la proposition révisée, ainsi que son importance, nécessitaient un nouvel avis, qu'il a rendu le 27 avril 2007<sup>(40)</sup>. Dans ses deux précédents avis sur la question, le CEPD a souligné qu'un cadre général est nécessaire pour la protection des données dans un espace de liberté, de sécurité et de justice, au sein duquel la coopération policière et judiciaire acquiert une importance croissante.

Dans son troisième avis, le CEPD adopte une attitude critique et recommande que la décision-cadre ne soit pas adoptée sans améliorations significatives, notamment en ce qui concerne les questions suivantes:

- extension du champ d'application pour inclure également le traitement des données nationales, afin que les données des citoyens fassent l'objet d'une protection appropriée même lorsqu'elles ne sont pas transmises à un autre État membre;
- limitation des finalités pour lesquelles les données à caractère personnel peuvent faire l'objet d'un traitement ultérieur, afin de respecter les principes fondamentaux de la convention 108;
- obligation d'assurer un niveau de protection adéquat pour les échanges avec les pays tiers, conformément à une norme commune de l'UE;
- garantie de la qualité des données, en établissant une distinction entre les données factuelles et les données non vérifiées, ainsi qu'entre les différentes catégories de personnes, telles que les témoins, les personnes déclarées coupables, etc.

En outre, le CEPD a recommandé au Conseil de ne pas négocier les nouvelles questions abordées dans la proposition — l'extension du champ d'application aux traitements de données effectués dans le cadre du troisième pilier par Europol et Eurojust et la création d'une nouvelle autorité de contrôle commune —, de crainte que certains autres éléments essentiels de la proposition ne soient pas suffisamment traités.

### Communication relative à la mise en application de la directive sur la protection des données

La communication de la Commission relative à la mise en application de la directive sur la protection des données réitère l'importance de la directive 95/46/CE, qui constitue une étape marquante en ce qui concerne la protection des données, et examine son contenu ainsi que sa mise en

<sup>(39)</sup> Document 7315/07 du Conseil du 13 mars 2007.

<sup>(40)</sup> Troisième avis du 27 avril 2007 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO C 139 du 23.6.2007, p. 1.

œuvre<sup>(41)</sup>. La conclusion centrale de la communication est que la directive ne devrait pas être modifiée. Sa mise en application devrait être améliorée au moyen d'autres instruments d'action, à caractère non contraignant pour la plupart.

L'avis rendu par le CEPD le 25 juillet 2007 confirme la conclusion principale de la Commission. Selon lui, il est plus opportun, à court terme, de se concentrer sur les améliorations à apporter à la mise en œuvre de la directive<sup>(42)</sup>. À plus long terme, toutefois, des modifications de la directive semblent inévitables. Le CEPD demande de fixer dès à présent une date précise pour l'examen de la directive en vue de l'élaboration des propositions destinées à apporter les modifications susmentionnées, ce qui inciterait certainement à entamer la réflexion sur les changements futurs. Il n'est pas nécessaire d'adopter de nouveaux principes, mais plutôt de prévoir d'autres dispositions administratives.

L'avis recense cinq perspectives quant aux modifications futures: mise en œuvre complète de la directive; interaction avec la technologie; respect de la vie privée à l'échelle mondiale et compétences; respect de la législation; impact du traité de Lisbonne.

En ce qui concerne la mise en application complète, le CEPD invite la Commission à envisager une série de recommandations, en particulier:

- dans certains cas, action législative spécifique au niveau de l'UE;
- recherche d'une meilleure mise en œuvre de la directive par le recours à des procédures d'infraction;
- utilisation d'une communication interprétative de l'instrument pour les questions suivantes: le concept de données à caractère personnel, la définition du rôle du responsable du traitement ou du sous-traitant, la détermination de la loi applicable, le principe de limitation de la finalité et les utilisations incompatibles, les motifs juridiques justifiant le traitement, notamment en ce qui concerne le consentement sans équivoque et l'équilibre des intérêts;
- large utilisation des instruments non contraignants, y compris ceux fondés sur la notion de «*privacy by design*» (prise en compte du respect de la vie privée dès la conception);
- présentation d'un document au groupe de l'article 29 donnant des indications claires concernant la répartition des rôles entre la Commission et le groupe.

<sup>(41)</sup> Communication de la Commission au Parlement européen et au Conseil du 7 mars 2007 intitulée «Suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données» [COM(2007) 87 final].

<sup>(42)</sup> Avis du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255 du 27.10.2007, p. 1.

## Statistiques communautaires sur la santé

Le 5 septembre 2007, le CEPD a rendu un avis sur la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail<sup>(43)</sup>.

La proposition a pour objectif d'établir le cadre de toutes les activités actuelles et prévisibles qui sont menées dans le domaine des statistiques de la santé publique et de la santé et de la sécurité au travail par Eurostat, les instituts nationaux de statistique et toutes les autres autorités nationales chargées de la fourniture de statistiques officielles dans ces domaines.

Les principales recommandations du CEPD portent sur la nécessité de prendre en compte les différences entre la protection des données et la confidentialité statistique, ainsi que les notions spécifiques y afférentes. En outre, la question du transfert de données à caractère personnel à des pays tiers ainsi que les périodes de conservation des données statistiques sont également analysées.

À la suite de discussions entre les services d'Eurostat et le CEPD, il a été décidé de procéder à un examen commun des procédures mises en place au sein d'Eurostat pour traiter des fichiers individuels à des fins statistiques, qui pourrait rendre nécessaire un contrôle préalable.

## Transporteurs par route

Le 12 septembre 2007, le CEPD a rendu un avis sur la proposition de règlement du Parlement européen et du Conseil établissant des règles communes sur les conditions à respecter pour exercer la profession de transporteur par route<sup>(44)</sup>.

Le règlement établit les conditions d'honorabilité, de capacité financière et de capacité professionnelle que les entreprises doivent remplir pour être autorisées à exercer la profession de transporteur routier. La proposition introduit des registres électroniques nationaux qui devront être interconnectés entre tous les États membres pour faciliter l'échange d'informations entre États membres. Elle contient une disposition spécifique sur la protection des données<sup>(45)</sup>.

Le CEPD recommande de modifier le règlement afin de:

- mieux définir des termes tels qu'«honorabilité»;
- lever les ambiguïtés relatives au rôle des autorités nationales;
- veiller à ce que les exigences de la directive 95/46/CE soient respectées.

<sup>(43)</sup> COM(2007) 46 final, JO C 295 du 7.12.2007, p. 1.

<sup>(44)</sup> JO C 14 du 19.1.2008, p. 1.

<sup>(45)</sup> COM(2007) 263 final du 6 juillet 2007.

### Mise en œuvre de l'initiative de Prüm

Le 19 décembre 2007, le CEPD a rendu un avis sur l'initiative allemande visant à établir les modalités d'application nécessaires en vue de la mise en œuvre de la décision du Conseil relative au traité de Prüm <sup>(46)</sup> (le CEPD avait déjà rendu un avis sur l'initiative visant à l'adoption de cette décision le 4 avril 2007).

Les modalités d'application et leur annexe revêtent une importance particulière, car elles définissent des aspects et des outils fondamentaux pour les échanges de données qui sont essentiels afin de fournir des garanties aux personnes concernées. En outre, en l'absence actuelle d'un cadre général au niveau de l'UE qui garantisse une protection harmonisée des données dans le secteur répressif, il convient d'accorder une attention spécifique à ces modalités.

Dans son avis, le CEPD formule notamment les recommandations suivantes:

- la combinaison de dispositions générales et de règles spécifiques relatives à la protection des données devrait garantir en même temps les droits des citoyens et l'efficacité des services répressifs lorsque la proposition entrera en vigueur;
- l'exactitude des consultations et des comparaisons des profils d'ADN et des empreintes digitales devrait être dûment prise en compte et constamment vérifiée, à la lumière également d'un système d'échange à plus grande échelle;
- il convient de faire en sorte que les autorités responsables de la protection des données puissent s'acquitter de manière appropriée de leur rôle de contrôle et de conseil tout au long des différentes étapes de la mise en œuvre.

### Communication sur l'identification par radiofréquence

Le 20 décembre 2007, le CEPD a rendu un avis sur la communication de la Commission relative à l'identification par radiofréquence <sup>(47)</sup> en Europe, qui a été publiée en mars 2007. Cet avis se penche sur l'utilisation croissante de puces RFID dans les produits de consommation et d'autres nouvelles applications ayant des incidences pour les personnes.

Le CEPD se félicite de la communication de la Commission sur la RFID, car elle aborde les principales questions posées

<sup>(46)</sup> Avis du 19 décembre 2007 sur l'initiative de la République fédérale d'Allemagne en vue de l'adoption d'une décision du Conseil concernant la mise en œuvre de la décision 2007/.../JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière.

<sup>(47)</sup> Avis du 20 décembre 2007 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique» [COM(2007) 96].

par le déploiement de la technologie RFID, tout en tenant compte des considérations relatives à la protection de la vie privée et des données. Le CEPD partage l'avis de la Commission selon lequel il convient, dans un premier temps, d'autoriser les instruments d'autoréglementation. Cependant, des mesures législatives complémentaires peuvent se révéler nécessaires pour réglementer l'utilisation de la RFID au regard de la protection de la vie privée et des données.

Le CEPD souligne que les systèmes RFID pourraient jouer un rôle essentiel dans le développement de la société de l'information européenne, mais que les avantages apportés par des garanties cohérentes en matière de protection des données devraient faciliter une large acceptation des technologies RFID. L'autoréglementation seule pourrait ne pas suffire à relever ce défi. Des instruments juridiques pourraient dès lors être nécessaires pour garantir la mise en place de solutions techniques permettant de réduire à un minimum les risques en matière de protection des données et de respect de la vie privée. En effet, la directive existante relative à la protection des données est suffisante dans un premier temps pour protéger la vie privée à condition toutefois que le cadre actuel soit effectivement appliqué. Il n'est pas utile de modifier les principes, mais des règles spécifiques complémentaires pourraient être requises pour obtenir des résultats satisfaisants.

Plus précisément, le CEPD invite la Commission à examiner les recommandations suivantes:

- fournir des orientations claires, en étroite coopération avec les parties intéressées, quant à la manière d'appliquer le cadre juridique actuel à l'environnement RFID;
- adopter une législation communautaire régissant les principales questions liées à l'utilisation de la RFID si le cadre juridique existant n'est pas effectivement appliqué;
- les mesures concernées devraient notamment établir que le principe du consentement préalable donné au point de vente constitue une obligation légale concrète et incontournable;
- recenser les «meilleures techniques disponibles», qui joueront un rôle décisif aux fins d'une adoption rapide du principe de la prise en compte du respect de la vie privée dès la conception.

### Décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives

La proposition de décision-cadre du Conseil prévoit l'obligation pour les transporteurs aériens de transmettre des données sur tous les passagers de leurs vols à destination ou en provenance d'un État membre, aux fins de la lutte contre le terrorisme et la criminalité organisée <sup>(48)</sup>.

<sup>(48)</sup> Proposition de décision-cadre du Conseil du 6 novembre 2007 relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives [COM(2007) 654 final].

Dans son avis du 20 décembre 2007 <sup>(49)</sup>, le CEPD souligne l'incidence majeure qu'aurait cette proposition sur les droits à la vie privée et à la protection des données des passagers des transports aériens. Tout en reconnaissant que la lutte contre le terrorisme est un objectif légitime, le CEPD estime que la nécessité et la proportionnalité de la proposition ne sont pas suffisamment établies. En outre, le CEPD se montre critique quant au manque de clarté concernant différents aspects de la proposition, en particulier le cadre juridique applicable, l'identité des destinataires des données à caractère personnel et les conditions de communication des données à des pays tiers.

Son avis est centré sur quatre questions essentielles et tire les conclusions suivantes:

- la légitimité du traitement: la proposition ne fournit pas d'éléments justificatifs suffisants pour appuyer et démontrer la légitimité du traitement de données;
- le cadre juridique applicable: d'importantes lacunes en matière de sécurité juridique sont constatées quant au régime de protection des données applicable aux différents acteurs intervenant dans le traitement des données à caractère personnel;
- l'identité des destinataires des données: la proposition ne précise pas l'identité des destinataires des données à caractère personnel, qui est essentielle pour évaluer les garanties que ces destinataires fourniront;
- le transfert de données à des pays tiers: il est de la plus haute importance que les conditions de la transmission des données PNR à des pays tiers soient cohérentes et soumises à un niveau de protection harmonisé.

Enfin, le CEPD recommande de ne pas adopter la décision avant l'entrée en vigueur du traité de Lisbonne afin qu'elle puisse suivre la procédure législative ordinaire prévue dans le nouveau traité et que le Parlement puisse y participer pleinement.

### 3.4. Observations

#### Sécurité et respect de la vie privée

Le 11 juin 2007, le CEPD a écrit aux ministres portugais de la justice et de l'intérieur pour demander à la présidence portugaise débutant le 1<sup>er</sup> juillet de veiller à ce que les initiatives du Conseil soient, avant leur adoption, précédées d'un examen approfondi de leurs incidences sur la protection des données. Il s'est déclaré préoccupé par le fait qu'un certain nombre d'accords prévoyant de nouvelles mesures de lutte contre le terrorisme ont été conclus sans que leurs répercussions sur les droits fondamentaux aient été pleinement prises en compte.

<sup>(49)</sup> Avis du 20 décembre 2007 sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives.



L'internet des objets: un environnement reposant sur des marqueurs d'identification par radiofréquence devra être respectueux de la vie privée.

Le CEPD a souligné que des messages tels que «pas de droit à la vie privée tant que la vie et la sécurité ne sont pas garanties» deviennent des slogans qui suggèrent que les droits et les libertés fondamentaux sont un luxe incompatible avec la sécurité. Il a exprimé sa préoccupation quant à cette approche négative; elle révèle un manque manifeste de compréhension du cadre juridique relatif aux droits de l'homme, qui a toujours permis la prise de mesures nécessaires et proportionnées pour combattre la criminalité et le terrorisme.

Cette approche ignore également les enseignements tirés des violations des droits fondamentaux commises dans le cadre de la lutte antiterroriste en Europe au cours des cinquante dernières années. Il ne devrait faire aucun doute qu'il est possible d'appliquer des mesures antiterroristes efficaces tout en respectant les droits fondamentaux. Dans le passé, des exemples dans différentes parties d'Europe ont montré que l'absence de protection des droits fondamentaux a donné lieu à des troubles incessants plutôt que de garantir la sécurité et la stabilité.

Dans la pratique, le CEPD veut faire en sorte que la protection des données soit considérée comme une condition de la légitimité — et même du succès — de toute nouvelle initiative dans ce domaine et démontrer les avantages qu'une protection efficace des données présente pour la sécurité et l'application des lois dans l'ensemble de l'Europe.

Le CEPD engage enfin le Conseil — ainsi que la Commission européenne — à le consulter sur toutes les questions concernant le traitement de données à caractère personnel.

Le large éventail d'avis transmis par le CEPD à la Commission à propos d'instruments de l'UE relevant du premier et du troisième pilier a permis d'améliorer la législation sur les plans de la légitimité et de l'efficacité.

Ces préoccupations ont été examinées lors d'une réunion entre le CEPD et le ministre portugais de la justice tenue le 17 septembre 2007, au cours de laquelle ce dernier a confirmé sa volonté de respecter, comme il se doit, le droit à la vie privée et les autres droits fondamentaux dans toutes les législations pertinentes.

### **Le traité de Lisbonne**

Dans une lettre adressée à la présidence de la Conférence intergouvernementale (CIG) le 23 juillet 2007, le CEPD a demandé l'inclusion de quelques points précis dans les dispositions relatives à la protection des données figurant dans le nouveau traité en vue d'améliorer le texte du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, ainsi que celui de la «déclaration sur la protection des données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale». La présidence de la CIG n'a malheureusement pas réagi aux suggestions du CEPD.

### **Progrès concernant la décision-cadre relative à la protection des données**

À la suite de son troisième avis sur la protection des données dans le cadre du troisième pilier, le CEPD a suivi de près les progrès réalisés dans le débat politique sur cet instrument législatif capital. Il a contacté la présidence portugaise pour lui donner des conseils sur certains points essentiels de la proposition. Le 16 octobre 2007, le CEPD a également formulé des observations concernant quelques points importants mais plus techniques à ne pas négliger au stade de la mise au point de la décision-cadre du Conseil.

En particulier, le CEPD a recommandé:

- de tenir compte du niveau minimal de protection fourni par la convention 108, notamment en ce qui concerne le traitement des données sensibles;
- de préciser le rapport entre la limitation des finalités pour lesquelles les données à caractère personnel sont collectées et la possibilité pour les services répressifs de les utiliser dans certains cas de manière incompatible avec ces finalités;
- de garantir un droit d'accès intégral aux données à caractère personnel, surtout en cas de décisions automatiques;
- de garantir le rôle consultatif des autorités responsables de la protection des données, notamment par le biais d'un forum au niveau de l'UE au sein duquel ces autorités pourraient coordonner leurs activités.

Le CEPD a également été invité à présenter sa position devant la commission des libertés civiles, de la justice et des

affaires intérieures du Parlement européen. En 2008, il continuera à suivre l'avancement de cette proposition et restera disposé à formuler de nouveaux avis à son sujet.

### **Contrôle de l'acquisition et de la détention d'armes**

Dans une lettre datée du 31 octobre 2007 et adressée au rapporteur du Parlement européen chargé de la question, le CEPD a réagi aux évolutions intervenues dans la procédure législative concernant la proposition de directive relative au contrôle de l'acquisition et de la détention d'armes<sup>(50)</sup>.

Ces évolutions ont soulevé une importante question liée à la protection des données, essentiellement à la suite d'un amendement figurant dans le rapport du rapporteur. Cet amendement prévoit l'établissement, dans chaque État membre, d'un système de fichiers informatisé et centralisé dans lequel plusieurs données seront conservées pendant au moins vingt ans.

Dans sa lettre, le CEPD évoque aussi plusieurs préoccupations concernant la conformité du système avec la directive 95/46/CE.

### **Règlement «Rome II» sur la loi applicable aux obligations non contractuelles**

Le 28 février 2007, le CEPD a écrit aux présidents du Parlement européen, du Conseil et de la Commission pour leur faire part de ses doutes et de ses préoccupations concernant l'article 7 bis (atteintes à la vie privée et aux droits de la personnalité) proposé dans la résolution législative du Parlement sur la position commune adoptée par le Conseil en vue de l'adoption du règlement du Parlement et du Conseil sur la loi applicable aux obligations non contractuelles (Rome II).

En effet, cet article aurait pu engendrer certaines incohérences avec la directive 95/46/CE. Premièrement, il n'était pas possible de déterminer avec certitude s'il était destiné à porter sur les violations des règles juridiques relatives aux traitements de données à caractère personnel figurant dans la directive et dans les instruments connexes. Le CEPD a fait observer que, si ce nouvel article 7 bis s'appliquait aux violations des règles juridiques établies dans la directive, cela signifiait qu'il adoptait une approche différente de celle prévue à l'article 4 de la directive en ce qui concerne la loi applicable.

Deuxièmement, le CEPD a exprimé un certain nombre de préoccupations plus détaillées relatives à la seule partie de l'article 7 bis mentionnant explicitement la notion de «données à caractère personnel». Il était difficile de déterminer si ce paragraphe aurait concerné les traitements de données en général ou uniquement ceux effectués par un organisme de radiodiffusion. En outre, le texte du paragraphe 3 présentait

<sup>(50)</sup> Lettre concernant la proposition de directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes, datée du 31 octobre 2007.

certaines incohérences terminologiques par rapport à la directive.

Le CEPD a suggéré l'adoption d'une approche plus prudente lors des prochaines étapes législatives afin d'obtenir une vision claire des incidences que pourrait avoir le texte proposé sur la législation existante en matière de protection des données et également d'éviter les problèmes potentiels brièvement décrits dans sa lettre.

Le règlement a été adopté le 11 juillet 2007 <sup>(51)</sup>. L'article 7 bis a été supprimé. Une clause de révision a été introduite à l'article 30, paragraphe 2, en vertu de laquelle une étude relative à la loi applicable aux obligations non contractuelles découlant des atteintes à la vie privée et aux droits de la personnalité doit être présentée par la Commission au plus tard le 31 décembre 2008.

### 3.5. Interventions devant la Cour de justice

Le CEPD utilise un autre instrument pour remplir son rôle de conseiller auprès des institutions de l'UE: l'intervention dans les affaires portées devant la Cour de justice des Communautés européennes, en vertu de l'article 47, paragraphe 1, point i), du règlement (CE) n° 45/2001. Cet instrument comprend des interventions devant le Tribunal de première instance et devant le Tribunal de la fonction publique. Son champ d'application a été défini par la Cour de justice dans ses ordonnances du 17 mars 2005 relatives au transfert de données PNR.

Le 12 septembre 2007, dans son ordonnance concernant l'affaire C-73/07 (*Satakunnan Markkinapörssi et Satamedia*), le président de la Cour de justice a précisé que la compétence du CEPD ne porte pas sur les procédures préjudicielles. Le CEPD avait présenté une demande d'intervention dans cette affaire en ce qui concerne «les traitements de données à caractère personnel effectués aux seules fins de journalisme» prévus par la directive 95/46/CE.

Le 8 novembre 2007, le Tribunal de première instance a rendu son arrêt dans l'affaire T-194/04 (*Bavarian Lager/Commission*), l'une des trois affaires concernant le lien entre l'accès du public aux documents et la protection des données dans lesquelles le CEPD est intervenu en 2006. Cet arrêt marque une étape importante dans les débats portant sur cet équilibre.

Le Tribunal de première instance a annulé la décision de la Commission de refuser l'accès complet au procès-verbal d'une réunion organisée par la Commission, comportant les noms des participants à cette réunion. Le Tribunal a estimé que la divulgation des noms des représentants d'un organe collectif ne portait pas atteinte à la protection de leur vie privée et de leur intégrité.

<sup>(51)</sup> JO L 199 du 31.7.2007, p. 40.

Le CEPD était intervenu dans l'affaire pour soutenir l'auteur d'une demande d'accès et avait défendu une position qui a été en substance confirmée par le Tribunal de première instance. En janvier 2008, la Commission a formé un recours devant la Cour de justice.

Une autre affaire portant sur la base juridique de la directive 2006/24/CE sur la conservation de données (affaire C-301/06, *Irlande/Parlement et Conseil*), pour laquelle le CEPD avait présenté une demande d'intervention en 2006, est toujours pendante devant la Cour de justice. En 2007, le CEPD a présenté des observations écrites.

Enfin, en décembre 2007, le CEPD a présenté une demande d'intervention devant le Tribunal de première instance dans l'affaire T-374/07 (*Pachtitis/Commission et EPSO*). Cette affaire concerne l'accès d'une personne aux questions qui lui ont été posées et aux réponses qu'elle a données lorsqu'elle a participé à un concours général visant à établir une liste de réserve de recrutement par les institutions européennes.

### 3.6. Autres activités

#### L'accord conclu avec les États-Unis sur les données PNR

Le CEPD a été étroitement associé au processus qui a conduit à l'accord entre l'UE et les États-Unis sur la question des données PNR, ainsi qu'aux différentes activités menées dans le prolongement de la conclusion du nouvel accord en juillet 2007.

Premièrement, le CEPD a formulé des observations sur le mandat de négociation, dans le respect intégral de l'impératif de confidentialité. Deuxièmement, il a participé activement aux activités du groupe de l'article 29 (notamment à l'élaboration d'un document de stratégie sur les données des passagers) et à l'organisation, au Parlement européen, d'un atelier destiné à faire mieux connaître les différents aspects de l'accord. Il a également exposé ses vues sur l'accord proposé en plusieurs occasions, par exemple en témoignant (par écrit et oralement) devant la commission sur l'Union européenne de la Chambre des lords.

À la suite de la conclusion de l'accord, le CEPD a participé, avec d'autres membres du groupe de l'article 29, à l'analyse du nouvel accord. Dans un avis adopté par le groupe le 17 août 2007, des préoccupations ont été exprimées quant au fait que les garanties prévues par le nouvel accord avaient été amoindries par rapport à celles figurant dans le rapport précédent.

Parmi les questions suscitant une inquiétude particulière figuraient le nombre et la qualité des données transmises, le nombre accru de destinataires, le manque de clarté concernant les finalités pour lesquelles les données peuvent être utilisées et les conditions de réexamen du système. Étant donné que le CEPD partageait entièrement les vues exprimées par le groupe, il n'a pas rendu d'avis.

Avec la contribution active du CEPD, le groupe s'est également penché sur les conditions d'information des passagers au moment de l'achat d'un billet d'avion. Un avis adopté le 15 février 2007 <sup>(52)</sup> contient des conseils à l'intention des compagnies aériennes quant aux informations données par téléphone, en personne et sur l'internet. Des modèles de notes d'information ont été établis pour faciliter cette information ainsi que pour garantir la cohérence des informations fournies dans l'ensemble de l'UE.

### Mesures d'exécution relatives au SIS II

Les instruments juridiques concernant un nouveau système d'information Schengen (SIS II) chargent la Commission d'établir les mesures d'exécution, et notamment d'élaborer le manuel Sirene pour le SIS II.

Ce manuel comprend certaines des règles nécessaires au bon fonctionnement du SIS II qui ne peuvent être couvertes de manière exhaustive par les instruments juridiques en raison de leur caractère technique, de leur niveau de détail ou parce qu'elles requièrent une mise à jour régulière. Elles complètent le cadre juridique. Étant donné que ces mesures sont susceptibles d'avoir une incidence sur les droits fondamentaux, le CEPD a été consulté de façon informelle.

Dans les observations qu'il a transmises à la Commission le 7 septembre 2007, le CEPD a abordé plusieurs questions, telles que:

- la communication des «informations complémentaires»: des précisions étaient requises concernant la notion d'«informations complémentaires» et la nécessité de prévoir ce type de communication dans le cadre du manuel Sirene;
- les mesures de sécurité: le CEPD a pris en considération le niveau élevé de sécurité requis par l'article 10, paragraphe 1, des instruments juridiques et a formulé plusieurs suggestions visant à renforcer les exigences en matière de sécurité, et notamment de sécurité informatique;
- d'autres questions, notamment: l'archivage, la suppression automatique des données, le changement de finalité d'un signalement, les demandes d'accès aux données ou de rectification des données, la mise en relation des signalements, les procédures prévues à l'article 25 de la convention de Schengen et les statistiques.

Ces observations informelles devaient initialement être suivies d'un avis du CEPD. Cependant, après avoir été examinées par le comité SIS-VIS le 12 septembre 2007, elles ont été prises en compte dans une mesure raisonnable. Les observations qui n'ont pas été retenues devraient faire l'objet d'une nouvelle discussion destinée à étudier la possibilité de les inclure dans une version révisée des mesures d'exécution.

<sup>(52)</sup> Avis 2/2007 concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record — PNR) aux autorités américaines (WP 132).

### Vers l'utilisation de statistiques

Le 5 septembre 2007, le CEPD a rendu un avis sur une proposition relative aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail (voir le point 3.3.2). Dans ses conclusions, le CEPD a indiqué qu'il convenait de procéder à un examen conjoint des opérations de traitement mises en place par Eurostat lorsque celui-ci traite des fichiers individuels à des fins statistiques, cet examen pouvant conclure à la nécessité d'un contrôle préalable.

Selon le CEPD, cet examen conjoint devrait comprendre une analyse des ensembles minimaux de données qui sont exigés pour chaque opération de traitement, ainsi qu'une analyse des opérations de traitement mises en œuvre par Eurostat. Depuis lors, plusieurs contacts ont été établis avec les services concernés d'Eurostat afin de réaliser cet examen conjoint. L'avis 4/2007 du groupe de l'article 29 sur le concept de données à caractère personnel servira de document de réflexion dans ce contexte.

Dans le même temps, le CEPD est consulté sur une proposition de règlement du Parlement européen et du Conseil relatif aux statistiques européennes. Cette consultation devrait se dérouler parallèlement à l'examen conjoint, afin que le CEPD puisse tirer des conclusions générales sur l'utilisation de statistiques.

### Système de coopération en matière de protection des consommateurs et système d'information du marché intérieur

Le CEPD a consacré une grande attention aux aspects liés à la protection des données de deux systèmes informatiques à grande échelle pour l'échange d'informations entre les États membres: le système de coopération en matière de protection des consommateurs (SCPC) et le système d'information du marché intérieur (IMI).

Le SCPC est une base de données électronique gérée par la Commission européenne aux fins de l'échange d'informations entre les autorités chargées de la protection des consommateurs dans les États membres et à la Commission, conformément au règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs <sup>(53)</sup>.

L'IMI est un autre système informatique à grande échelle géré par la Commission afin de faciliter les échanges d'informations entre les autorités compétentes dans les États membres dans le domaine de la législation relative au marché intérieur. Actuellement, les échanges d'informations dans le cadre de l'IMI sont effectués uniquement en application de la directive 2005/36/CE («directive relative aux qualifi-

<sup>(53)</sup> Règlement (CE) n° 2006/2004 du Parlement européen et du Conseil du 27 octobre 2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO L 364 du 9.12.2004, p. 1.

cations professionnelles»)<sup>(54)</sup> et de la directive 2006/123/CE («directive relative aux services»)<sup>(55)</sup>.

Le CEPD a, dans un premier temps, participé aux travaux d'un sous-groupe ad hoc du groupe de l'article 29, qui ont débouché sur l'adoption par le groupe de deux avis sur le SCPC et l'IMI<sup>(56)</sup>. Il a joué le rôle de rapporteur en ce qui concerne l'avis sur le SCPC. Par la suite, à l'automne 2007, le CEPD a participé activement à l'élaboration:

- d'une décision de la Commission modifiant les dispositions d'application relatives au SCPC;
- d'une nouvelle décision de la Commission sur les aspects de l'IMI liés à la protection des données.

Le CEPD s'est déclaré favorable à la mise en place de systèmes électroniques pour l'échange d'informations. De tels systèmes rationalisés peuvent non seulement améliorer l'efficacité de la coopération, mais également contribuer à garantir le respect des législations applicables en matière de protection des données; en effet, ils fournissent un cadre clair indiquant quelles sont les informations qui peuvent être échangées, avec qui et dans quelles conditions.

Cependant, la création d'un système électronique centralisé peut également présenter certains risques. Parmi les plus importants figure le fait que les données échangées peuvent être plus nombreuses et transmises à une plus large échelle que ce qui est strictement requis aux fins d'une coopération efficace, et que les données, y compris des données potentiellement périmées et inexacts, peuvent rester dans le système électronique plus longtemps que nécessaire. La sécurité d'une base de données accessible dans vingt-sept États membres est également un point sensible, car le système n'est sûr que dans la mesure où le lien le plus faible au sein du réseau le permet. C'est pourquoi le CEPD a recommandé que les préoccupations relatives à la protection des données soient intégralement prises en compte, tant au niveau opérationnel que dans des décisions de la Commission juridiquement contraignantes concernant chaque système.

### Groupe des parties intéressées par la RFID

En mai 2007, le CEPD a été invité par la Commission européenne à participer, en tant qu'observateur, à un groupe d'experts ou de parties intéressées par la RFID mis en place pour une durée de trois ans. La mission du groupe est d'aider la Commission à:

- élaborer une recommandation (sa principale activité en 2007);

<sup>(54)</sup> Directive 2005/36/CE du Parlement européen et du Conseil du 7 septembre 2005 relative à la reconnaissance des qualifications professionnelles, texte consolidé publié au JO L 271 du 16.10.2007, p. 18.

<sup>(55)</sup> Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur, JO L 376 du 27.12.2006, p. 36.

<sup>(56)</sup> WP 139 et WP 140 du 20 septembre 2007, publiés sur le site internet du groupe.



Données relatives aux passagers: elles sont utilisées dans le cadre des vols, mais également pour la recherche de criminels.

- mettre au point des orientations concernant le mode de fonctionnement des applications RFID;
- évaluer l'opportunité de nouvelles mesures législatives;
- analyser la nature et les effets de l'évolution vers un «internet des objets» que l'on observe actuellement;
- soutenir l'initiative de la Commission visant à promouvoir des campagnes de sensibilisation.

Le CEPD a participé activement aux cinq réunions qui ont été organisées en 2007 et fourni une analyse pour alimenter les débats menés au sein du groupe. Il continuera à contribuer aux travaux du groupe en 2008, notamment en ce qui concerne le défi posé par l'«internet des objets» et les aspects de la RFID liés à la gouvernance.

### Groupe d'experts en matière de conservation des données

Le CEPD a participé aux différentes réunions du groupe d'experts en matière de conservation des données. Aux termes du considérant 14 de la directive 2006/24/CE sur la conservation des données, «les technologies liées aux communications électroniques progressent rapidement, et les exigences légitimes des autorités compétentes peuvent évoluer». Afin d'obtenir des conseils et d'encourager la mise en commun des bonnes pratiques à cet égard, la Commission européenne a l'intention d'instituer un groupe composé des services répressifs des États membres, des associations du secteur des communications électroniques, de représentants du Parlement européen et des autorités chargées de la protection des données, y compris le Contrôleur européen de la protection des données.

Ce groupe sera officiellement créé en 2008, mais s'est déjà réuni en 2007, à trois reprises.

## 3.7. Nouvelles évolutions

Les cinq perspectives quant aux modifications futures recensées dans l'avis du CEPD sur la communication de la Commission relative à la mise en application de la directive sur la protection des données (interaction avec la technologie, impact du traité de Lisbonne, respect de la législation, respect de la vie privée à l'échelle mondiale et compétences et mise en œuvre complète de la directive) serviront de programme pour les activités futures du CEPD.

### 3.7.1. Interaction avec la technologie

Dans son rapport annuel 2005, le CEPD a mis en évidence trois grandes évolutions technologiques sur lesquelles la société de l'information tablera de plus en plus son développement:

- 1) un environnement quotidien fait de points d'accès au réseau omniprésents;
- 2) une bande passante presque illimitée;
- 3) une capacité de stockage infinie.

Depuis ce rapport, ces évolutions technologiques émergentes ont commencé à avoir des implications concrètes, qu'il est nécessaire de suivre de près car elles devraient avoir une incidence non négligeable sur le cadre juridique de l'UE en matière de protection des données. Certaines de ces implications sont évoquées ci-après.

#### Tendances

En 1984, William Gibson <sup>(57)</sup> a décrit le «cyberespace» comme un environnement nouveau et, en fin de compte, parallèle de la société de l'information. Plus de vingt ans plus tard, la société de l'information ne peut plus être considérée comme un univers parallèle, mais constitue plutôt une part croissante, numérisée et intégrée de la vie quotidienne de chaque individu ou presque.

Comme l'indique un article récent paru dans *Firstmonday* <sup>(58)</sup>, un journal en ligne fondé sur le principe de l'évaluation par les pairs, l'utilisateur/l'individu est considéré comme un «producteur» essentiel des nouvelles applications qui peuplent le web 2.0, ces applications étant alimentées par ses données à caractère personnel, ainsi que par ses interactions sociales et professionnelles avec les autres.

#### Augmentation du nombre d'applications «sociales»

De plus en plus, la vie sociale des individus est numérisée au moyen d'applications gérées par les utilisateurs et alimentées par des données dont la plupart sont à caractère personnel. Ces applications, qui donnent lieu à la mise en place de

<sup>(57)</sup> Gibson, William, *Neuromancer*, édition Ace, juillet 1984.

<sup>(58)</sup> [http://www.firstmonday.org/ISSUES/issue12\\_3/pascu/](http://www.firstmonday.org/ISSUES/issue12_3/pascu/).



Les statistiques peuvent inclure des informations à caractère personnel.

réseaux sociaux en ligne, doivent leur succès au nombre d'utilisateurs inscrits, au grand nombre de données précises relatives aux profils stockés et, bien entendu, à leur capacité à renforcer les liens entre individus et contenus.

Le CEPD considère ce nouveau type d'applications comme une évolution technologique qui aura probablement d'importantes répercussions sur la protection des données. Il reste à déterminer si le cadre juridique en vigueur dans l'UE en matière de protection des données assurera une protection suffisante. Une attention particulière doit être accordée à la notion de «responsable du traitement» (quelle est sa signification si les utilisateurs finals sont les principaux acteurs du traitement des données?), à l'applicabilité du règlement et à la notion, de plus en plus relative, de lieu du traitement. Le CEPD salue le premier document d'orientation présenté en 2007 par l'Agence européenne chargée de la sécurité des réseaux et de l'information, qui aborde certaines questions relatives à la sécurité et formule des recommandations concernant les applications «sociales» <sup>(59)</sup>.

Les applications sociales et les réseaux sociaux trouvent également leurs fondements techniques dans un environnement professionnel plus ancien, axé sur le développement d'applications à distance et d'installations de stockage lointaines, qui s'appuient sur des supercentres de données et des fermes de serveurs, interconnectés dans le cadre d'un «nuage» (*cloud computing*) <sup>(60)</sup>.

<sup>(59)</sup> «Security issues and recommendations for online social networks» (Questions de sécurité et recommandations pour les réseaux sociaux en ligne), octobre 2007, document d'orientation n° 1, ENISA ([http://www.enisa.europa.eu/doc/pdf/deliverables/enisa\\_pp\\_social\\_networks.pdf](http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf)).

<sup>(60)</sup> [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing).

### *Centres de données, virtualisation et stockage de données à distance*

Compte tenu des trois grandes évolutions technologiques susmentionnées, qui rendent leur développement possible, les centres de données pourraient annoncer la fin du système de bureau dans le cadre duquel les données, et plus particulièrement les données à caractère personnel, ont été traitées jusqu'à présent. Des applications de stockage des données à distance et des applications en ligne commencent déjà à apparaître, mais il faut encore examiner le cadre de protection des données applicable, ainsi que les conditions requises pour qu'il soit correctement appliqué. Comme pour les réseaux sociaux, la définition «lieu» du traitement et l'identification du responsable du traitement en cas de ressources informatiques distribuées sont de plus en plus problématiques.

Lorsque le traitement de données à caractère personnel, stockées sur des installations utilisant un système poste à poste, sera diffusé par le biais d'un «nuage», il sera de plus en plus difficile, dans le cadre de la mise en œuvre traditionnelle du cadre de l'UE en matière de protection des données, d'appliquer efficacement les principes qui sous-tendent ce cadre.

Ainsi qu'il l'a souligné dans son avis sur la mise en application de la directive sur la protection des données <sup>(61)</sup>, le CEPD estime que, au vu de ces évolutions technologiques et afin de préserver les innovations et d'encourager de nouvelles interactions sociales et de nouveaux modèles commerciaux, il semble inévitable de modifier ladite directive, tout en conservant ses principes fondamentaux. D'autres dispositifs administratifs pourraient s'imposer, qui, d'une part, seraient efficaces et appropriés dans le cadre d'une société en réseau et, d'autre part, réduiraient au minimum les coûts administratifs.

### **Recherche et développement (R & D)**

Puisque les exigences en matière de respect de la vie privée et de protection des données doivent être mises en évidence et appliquées dès que possible dans le cycle de vie des nouvelles évolutions technologiques, le CEPD est d'avis que les efforts consentis par l'UE en matière de R & D sont l'occasion d'atteindre ces objectifs et que le principe de «*privacy by design*» (prise en compte du respect de la vie privée lors de la conception) devrait faire partie intégrante de ces initiatives. Le CEPD a donc entrepris plusieurs actions en vue de mettre en œuvre ce principe en 2007.

#### *Examen des propositions relevant du 7<sup>e</sup> programme-cadre*

En juillet 2007, à la demande de la Commission, le CEPD a examiné certaines propositions relevant du 7<sup>e</sup> programme-cadre pour des actions de recherche et de développement

technologique, en réponse au premier appel d'offres concernant les technologies de l'information et de la communication (TIC). Il a formulé des conseils en matière de protection des données concernant les propositions pour lesquelles tous les seuils avaient déjà été atteints.

#### *Document stratégique sur la recherche et le développement*

Au début de 2008, le CEPD a adopté un document stratégique décrivant le rôle que l'institution pourrait jouer dans le cadre des projets de R & D relevant du 7<sup>e</sup> programme-cadre. Ce document présente les critères de sélection des projets qui peuvent faire l'objet d'une action du CEPD et décrit la manière dont le CEPD peut contribuer à ces projets. Le CEPD ayant le statut d'autorité indépendante, sa participation en tant que partenaire d'un groupement d'entreprises ne peut pas être envisagée.

### **3.7.2. Faits nouveaux dans les domaines politique et législatif**

#### **Impact du traité de Lisbonne**

Le cadre juridique de l'Union européenne va changer avec l'entrée en vigueur du traité de Lisbonne. Ce traité aura également des conséquences sur le rôle de conseiller du CEPD et sur les activités qu'il exerce dans ce domaine. Il déterminera un nouveau contexte pour ces activités, ce qui aura un impact spécifique sur les propositions de législation relatives à l'échange de données à caractère personnel et à la protection de ces données à des fins répressives.

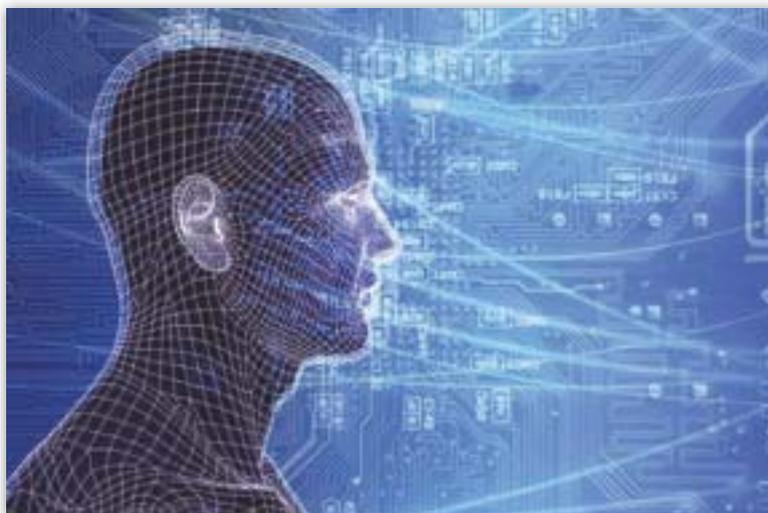
Les questions que le CEPD devra examiner en 2008 sont notamment les suivantes:

- Comment agir pendant la période de transition? Les actes importants ne devraient pas être adoptés avant la mise en place du nouveau traité (avec le vote à la majorité qualifiée, la procédure de codécision et la possibilité de recourir aux procédures d'infraction).
- Quel est l'impact du nouveau traité dans des domaines où des personnes privées interviennent dans des activités répressives?
- Est-il nécessaire de modifier la directive 95/46/CE et le règlement (CE) n° 45/2001?

#### **Respect de la législation**

Le CEPD s'attend à ce que les activités législatives relatives aux besoins accrus en matière de stockage et d'échange de données à caractère personnel à des fins répressives se poursuivent. Dans son approche concernant ces activités législatives, le CEPD continuera à analyser la nécessité desdites activités, qui viendraient s'ajouter à une législation existante qui n'a souvent même pas été pleinement mise en œuvre.

<sup>(61)</sup> Examiné au point 3.3 du rapport annuel.



Les principes de la protection des données sont également applicables à l'espace social numérique.

Il pourrait se révéler nécessaire de définir d'autres approches, assorties d'autres solutions pour réagir aux menaces à l'encontre de la société. La pleine mise en œuvre de la législation existante devrait toujours être un facteur important. Il convient de tenir dûment compte des risques associés au fait que de nouvelles lois pourraient contribuer à l'émergence d'une «société de la surveillance».

Une autre question sur laquelle le CEPD doit se pencher est le cadre de la protection des données, qui peut être décrit comme un patchwork (et ce éventuellement aussi en raison de l'adoption de la décision-cadre du Conseil) susceptible d'intervenir au début de 2008. Ce cadre est insuffisant et les règles applicables aux situations spécifiques n'apparaissent pas clairement. Cela s'applique également aux voies de recours dont dispose la personne concernée.

### Respect de la vie privée à l'échelle mondiale et compétences

Dans ce contexte, il est utile de garder à l'esprit les développements mentionnés ci-dessous:

- L'échange d'informations par le biais de sources ouvertes telles que l'internet devient de plus en plus courant. Il n'est pas évident de déterminer dans quelle mesure la législation de l'UE est applicable et exécutoire à l'égard de l'internet, également du fait que les prestataires de services sont souvent basés à l'extérieur du territoire de l'UE. À titre d'exemple, nous pouvons mentionner des moteurs de recherche tels que Google ou Yahoo.
- Le transfert de données à caractère personnel vers des pays tiers à des fins répressives et même l'accès par des autorités de pays tiers à des données au sein du territoire de l'UE prennent une importance croissante. Le nombre de pays tiers demandant ce transfert ou cet accès augmente, par exemple en ce qui concerne les données des dossiers passagers.

- Il n'existe pas de consensus sur le plan mondial concernant des normes communes en matière de vie privée. Les premières étapes sur la voie d'une approche transatlantique commune ont été franchies récemment.

Comme indiqué dans l'avis du CEPD relatif à la mise en application de la directive sur la protection des données, le défi consistera à trouver des solutions pratiques qui concilient la nécessité de protéger les citoyens européens concernés et les limitations territoriales de l'Union européenne et de ses États membres.

Un deuxième défi consistera à déterminer la manière de maintenir le niveau (élevé) de protection au sein de l'UE, également dans les relations de celle-ci avec des pays tiers: dans quelle mesure devrions-nous promouvoir ou abandonner nos propres normes et dans quelle mesure devrions-nous négocier des normes communes?

### Mise en œuvre complète

Comme expliqué dans l'avis du CEPD relatif à la mise en application de la directive sur la protection des données (voir le point 3.3), la mise en œuvre complète inclut un certain nombre de mesures qui joueront également un rôle important pour les travaux du CEPD dans les années à venir. En tout état de cause, les travaux sur les communications inter-prétatives constitueront une question essentielle. Ces communications peuvent contribuer à harmoniser davantage les lois sur la protection des données dans les États membres et révèlent également des thèmes susceptibles de faire l'objet de modifications futures de la directive.

Enfin, le CEPD participera activement à des discussions sur d'éventuelles modifications futures de la directive sur la protection des données et en lancera même à certaines occasions.

Il convient de garder à l'esprit que des modifications futures pourraient avoir des implications non seulement pour la directive 95/46/CE, mais également pour des instruments connexes, tels que la directive 2002/58/CE et le règlement (CE) n° 45/2001.

## 4. Coopération

### 4.1. Groupe de l'article 29

Le groupe de l'article 29 a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif indépendant sur la protection des données à caractère personnel, agissant dans le cadre de ladite directive <sup>(62)</sup>. Sa mission, décrite à l'article 30, peut être résumée comme suit:

- donner à la Commission européenne un avis autorisé au nom des États membres sur les questions relatives à la protection des données;
- promouvoir l'application uniforme des principes généraux de la directive dans tous les États membres, au moyen de la coopération entre les autorités de contrôle compétentes en matière de protection des données;
- conseiller la Commission sur toute mesure communautaire ayant une incidence sur les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel;
- formuler des recommandations destinées au grand public et, en particulier, aux institutions communautaires sur toute question concernant la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté européenne.

Le CEPD est membre du groupe de l'article 29 depuis le début de l'année 2004. Selon l'article 46, point g), du règlement (CE) n° 45/2001, il participe aux activités du groupe. Le CEPD estime qu'il s'agit d'une enceinte très importante pour la coopération avec les autorités nationales de contrôle. Il va aussi de soi que le groupe joue un rôle central dans la mise en œuvre homogène de la directive et l'interprétation de ses principes généraux.

Conformément à son programme de travail 2006-2007 et avec le ferme soutien du CEPD, le groupe a axé ses travaux sur un certain nombre de questions stratégiques en vue de

<sup>(62)</sup> Le groupe est composé de représentants des autorités nationales de contrôle de chaque État membre, d'un représentant de l'autorité créée pour les institutions et organes communautaires (c'est-à-dire le CEPD) et d'un représentant de la Commission. Cette dernière assure également son secrétariat. Les autorités nationales de contrôle de l'Islande, du Liechtenstein et de la Norvège (partenaires EEE) sont représentées en tant qu'observatrices.

contribuer à une compréhension commune des principales dispositions et d'en assurer une meilleure mise en œuvre. Le groupe a également amélioré la communication extérieure relative à son propre fonctionnement, en élaborant divers documents importants, parmi lesquels figurent:

- le document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques, adopté le 15 février 2007 (WP 131);
- l'avis 2/2007 concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record — PNR) aux autorités américaines, adopté le 15 février 2007 (WP 132);
- la politique révisée et mise à jour pour promouvoir la transparence des activités du groupe de travail établi par l'article 29 de la directive 95/46/CE, adoptée le 15 février 2007 (WP 135);
- l'avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007 (WP 136).

Le groupe a rendu un certain nombre d'avis sur des propositions de législation ou des documents similaires. Dans certains cas, ces questions ont également fait l'objet d'avis du CEPD, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001. Si l'avis du CEPD est une étape obligatoire du processus législatif de l'UE, les avis du groupe sont aussi très utiles, notamment parce qu'ils peuvent attirer l'attention sur des points particuliers, présentant de l'intérêt sur le plan national.

Le CEPD se félicite des avis rendus par le groupe de l'article 29, qui allaient dans le même sens que ses propres avis. Dans un cas, le CEPD a développé, dans son avis, certains éléments figurant dans l'avis du groupe. Dans un autre cas, le CEPD a préféré collaborer plus étroitement encore dans le cadre d'un avis unique, sans formuler ses propres observations. Les avis cités ci-dessous sont des exemples de la synergie mise en place dans ce domaine entre le groupe de l'article 29 et le CEPD:

- avis 3/2007 sur la proposition de règlement du Parlement européen et du Conseil modifiant les instructions

consulaires communes adressées aux représentations diplomatiques et consulaires de carrière, en liaison avec l'introduction d'éléments d'identification biométriques et de dispositions relatives à l'organisation de la réception et du traitement des demandes de visa, adopté le 1<sup>er</sup> mars 2007 (WP 134) <sup>(63)</sup>;

- avis 5/2007 concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure, conclu en juillet 2007, adopté le 17 août 2007 (WP 138);
- avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives, présentée par la Commission le 6 novembre 2007, adopté le 5 décembre 2007 (WP 145) <sup>(64)</sup>.

Le CEPD et le groupe ont analysé en étroite collaboration deux nouveaux systèmes de grande ampleur relevant du premier pilier, pour lesquels les tâches de contrôle exercées aux niveaux communautaire et national exigent une coordination rigoureuse:

- avis 6/2007 concernant les questions de protection des données posées par le système de coopération en matière de protection des consommateurs (SCPC), adopté le 20 septembre 2007 (WP 139);
- avis 7/2007 sur les questions de protection des données liées au système d'information du marché intérieur (IMI), adopté le 20 septembre 2007 (WP 140).

Conformément à l'article 46, point f) i), du règlement (CE) n° 45/2001, le CEPD doit également coopérer avec les autorités nationales de contrôle dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes les informations utiles et en demandant ou en donnant toute aide utile à l'exécution de leurs tâches respectives. Cette coopération se met en place au cas par cas. Le traitement du cas SWIFT est resté un bon exemple de coopération multilatérale: le groupe de l'article 29 a contrôlé régulièrement le suivi de son avis adopté en 2006 <sup>(65)</sup> et a pu finalement constater des avancées notables en matière de respect de la législation (voir aussi le point 2.5).

La coopération directe avec les autorités nationales se révèle de plus en plus utile lorsqu'il est question de vastes systèmes internationaux tels qu'Eurodac, qui exigent une approche coordonnée en matière de contrôle (voir le point 4.3).

<sup>(63)</sup> Voir également l'avis rendu par le CEPD le 27 octobre 2006.

<sup>(64)</sup> Le groupe «Police et justice» (voir le point 4.4) a adopté cet avis le 18 décembre 2007. Voir également l'avis rendu par le CEPD le 20 décembre 2007.

<sup>(65)</sup> Avis 10/2006 sur le traitement des données à caractère personnel par la Society for Worldwide Interbank Financial Telecommunication (SWIFT), adopté le 22 novembre 2006 (WP 128).

## 4.2. Groupe «Protection des données» du Conseil

En 2006, les présidences autrichienne et finlandaise ont organisé un certain nombre de réunions du groupe «Protection des données» du Conseil. Le CEPD a salué cette initiative, qu'il considère comme un moyen de mieux assurer une approche horizontale des questions relevant du premier pilier, et a participé à plusieurs de ces réunions.

La présidence allemande a décidé de poursuivre sur la même base en organisant des débats sur les éventuelles initiatives de la Commission et d'autres sujets pertinents dans le cadre du premier pilier. En janvier 2007, elle a pris l'initiative d'envoyer aux États membres un questionnaire relatif à leur expérience dans le domaine de la directive 95/46/CE. Environ la moitié des délégations ont répondu aux questions. Les réponses obtenues ont confirmé que la directive est généralement appréciée, bien que les délégations aient aussi largement évoqué les problèmes potentiels et les solutions possibles. Néanmoins, la présidence allemande n'a pas dégagé de conclusions précises.

En mai 2007, la Commission a présenté ses communications relatives au suivi du programme de travail pour une meilleure mise en œuvre de la directive sur la protection des données, à la promotion de la protection des données grâce aux technologies renforçant la protection de la vie privée et à l'identification par radiofréquence (RFID). Deux de ces communications ont fait l'objet d'un avis du CEPD (voir le point 3.3). Les débats au sein du groupe du Conseil n'ont pas abouti à des conclusions divergentes.

À l'occasion de la première réunion organisée sous la présidence allemande, le CEPD a présenté ses priorités en matière de consultation sur les nouvelles législations (voir le point 3.2). C'est au cours de la deuxième réunion qu'il a soumis son rapport annuel 2006.

La présidence portugaise avait prévu une réunion du groupe, qui a dû être annulée. La présidence slovène a également prévu une réunion en mai 2008.

Le CEPD continue de suivre ces activités avec beaucoup d'intérêt et est disposé à donner des avis et à coopérer, le cas échéant.

## 4.3. Contrôle coordonné d'Eurodac

La coopération établie avec les autorités nationales chargées de la protection des données, afin d'instaurer une approche coordonnée pour le contrôle d'Eurodac, s'est développée rapidement depuis sa mise en place, il y a seulement quelques années.

Le groupe de coordination du contrôle d'Eurodac (ci-après dénommé «le groupe») est composé de représentants des autorités nationales chargées de la protection des données et du CEPD et s'est réuni trois fois, en mars, en juin et en

décembre 2007. Il a adopté des documents extrêmement utiles pour la mise en œuvre d'un contrôle coordonné, tandis que le CEPD réalisait, sur la même période, un audit de sécurité de la base de données centrale d'Eurodac (voir le point 2.10).

### Première inspection coordonnée

Lors de sa première réunion organisée en 2005, le groupe avait décidé de lancer des inspections, au niveau national, sur des éléments précis du système Eurodac. Les résultats devaient être compilés par le CEPD. La première inspection a été réalisée en 2006 et conclue au printemps 2007. Le rapport a été publié en juillet 2007 <sup>(66)</sup>.

Trois aspects importants — «recherches spéciales», «utilisation ultérieure» et «qualité des données» — ont été soigneusement examinés.

D'après le groupe, rien n'indique qu'il y a eu usage abusif du système Eurodac. Certains aspects, tels que l'information des personnes concernées, doivent néanmoins être améliorés.

Le rapport a été communiqué aux principaux acteurs institutionnels, au niveau de l'Union européenne, ainsi qu'aux organisations internationales et aux organisations non gouvernementales (ONG) chargées des questions d'asile et d'immigration. Cette inspection a eu une incidence notable sur le nombre des recherches spéciales, qui a sensiblement décliné dans tous les États membres.

Le CEPD considère que cette expérience positive a mis en évidence la bonne coopération au sein du groupe et sa capacité à faire la différence. Si cette expérience est importante, ce n'est pas seulement en termes de respect du droit des demandeurs d'asile à bénéficier de la protection de leurs données à caractère personnel, mais aussi parce qu'il s'agissait d'un exercice pilote d'une grande utilité pour d'autres systèmes d'information à grande échelle, tels que le SIS II.

### Formalisation des méthodes de travail

À l'origine, le groupe assurait le contrôle coordonné d'Eurodac de manière informelle, sur la base du règlement «Eurodac» (article 20) et de son expérience au sein d'autres instances. La nécessité d'une approche plus structurée s'est fait sentir, pour trois raisons principales:

- D'une part, le modèle de contrôle coordonné dans le cadre d'Eurodac est susceptible d'être utilisé à l'avenir pour d'autres systèmes. Les textes législatifs relatifs à ces systèmes prévoient un contrôle coordonné, les autorités concernées devant définir et élaborer leurs règles ou leurs méthodes de travail internes. Lancer la réflexion sur ces règles permettrait de disposer de plus de temps pour un développement progressif.

- Le recours aux «recherches spéciales» est légalement limité aux demandeurs d'asile et aux immigrants illégaux qui souhaitent accéder à leurs données personnelles. Le nombre de recherches effectuées variait considérablement d'un pays à l'autre, et il y avait des inquiétudes quant aux chiffres élevés pour certains pays. Le groupe a conclu que des erreurs initialement commises dans l'utilisation des recherches spéciales ont été corrigées.
- Les empreintes digitales Eurodac ne peuvent être utilisées que pour déterminer le pays qui est responsable d'une demande d'asile. Aucun abus n'a été décelé, en dépit du fait que certaines unités nationales Eurodac relèvent des forces de police et malgré une intensification générale de l'accès des services répressifs aux banques de données. Le groupe a également constaté que, dans certains pays, il était difficile d'identifier l'entité responsable du traitement des données à caractère personnel; le rapport recommande que des mesures soient prises pour remédier à ce problème.
- La qualité des empreintes digitales est une exigence fondamentale. La Commission européenne s'est inquiétée que 6 % des empreintes digitales soient rejetées en raison de leur mauvaise qualité. Le groupe a conclu que les pays concernés devraient prendre toutes les mesures nécessaires pour améliorer la qualité des empreintes, tant au niveau de la technologie utilisée (recours aux scanners) qu'à celui de la formation.

- D'autre part, le réexamen du système «Dublin» aboutira à des propositions législatives concernant Eurodac. Il est fort probable qu'une partie de la nouvelle législation portera sur le contrôle d'Eurodac. Dans ce cadre, il serait logique que le législateur européen suive le même schéma que celui prévu pour d'autres systèmes d'information à grande échelle. Eurodac pourrait ainsi bénéficier d'un contrôle coordonné sur le même modèle, y compris l'adoption de méthodes de travail formalisées, si nécessaire.
- Enfin, des pays non membres de l'Union européenne (l'Islande, la Norvège et la Suisse, par exemple) ont adhéré au système, notamment au modèle de contrôle, ou sont en passe de le faire. Ces pays ne sont pas couverts expressis verbis par le règlement «Eurodac»; il convient de fournir à leurs autorités chargées de la protection des données une description claire du modèle de contrôle auquel elles adhèrent.

<sup>(66)</sup> Voir le site du CEPD: onglet «Supervision», section «Eurodac».

Le CEPD a présenté une liste de points importants à examiner au cours de la réunion de mars. Après discussion, une proposition formelle de règlement intérieur a été analysée lors de la réunion de juin. Il a été convenu qu'il devait clarifier la situation tout en autorisant une certaine souplesse et qu'il ne devait pas être d'une lourdeur excessive. Le règlement intérieur a été adopté en décembre 2007.

### Activités futures

L'année 2007 a été marquée par plusieurs faits nouveaux et importants. D'une part, la Commission a publié en juin le rapport sur l'évaluation de la convention de Dublin, qui présentait une analyse du fonctionnement d'Eurodac et suggérait de nouvelles perspectives. De l'autre, une pression toujours plus forte s'exerce quant à l'octroi aux autorités répressives d'un accès aux données Eurodac. Ces deux aspects ont pu être observés dans le contexte du développement actuel de systèmes informatiques à grande échelle.

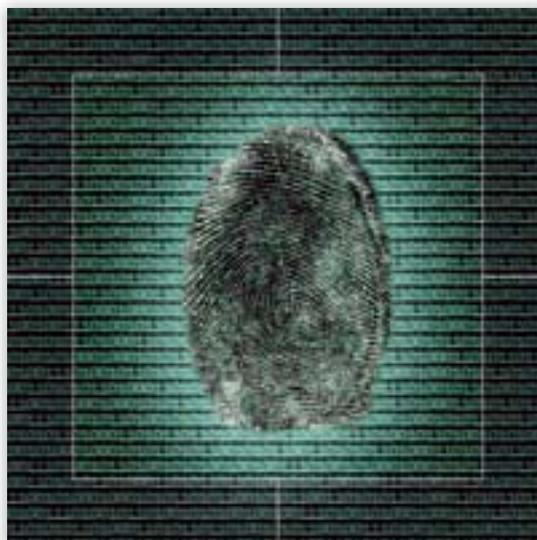
Le groupe a défini ses priorités dans le cadre de ces évolutions: un programme de travail a été adopté lors de la réunion de décembre. Le contrôle coordonné portera sur les éléments suivants: les informations à fournir aux personnes concernées, les empreintes digitales des enfants et l'utilisation de DubliNet. La question de l'effacement anticipé des données devrait aussi être examinée dans le courant de l'année 2008.

## 4.4. Troisième pilier

L'article 46, point f) ii), du règlement (CE) n° 45/2001 prévoit que le CEPD coopère avec les organes de contrôle de la protection des données institués en vertu du titre VI du traité sur l'Union européenne («troisième pilier») en vue d'améliorer «la cohérence dans l'application des règles et procédures dont ils sont respectivement chargés d'assurer le respect». Ces organes de contrôle sont les autorités de contrôle communes (ACC) de Schengen, d'Europol, d'Eurojust et du système d'information douanier. La plupart sont composés de représentants (en partie les mêmes) des autorités nationales de contrôle. En pratique, la coopération se fait avec les ACC concernées, avec l'aide du secrétariat commun à la protection des données travaillant au Conseil, et, plus généralement, avec les autorités nationales chargées de la protection des données.

La nécessité d'une coopération étroite entre les autorités nationales chargées de la protection des données et le CEPD s'est fait sentir ces dernières années avec l'augmentation des initiatives prises au niveau européen pour lutter contre le terrorisme et la criminalité organisée, dont diverses propositions relatives à l'échange de données à caractère personnel.

En 2007, les travaux ont été principalement axés sur deux questions importantes. La première était la discussion sur la



Eurodac a été créé pour comparer les empreintes digitales des demandeurs d'asile et des immigrants clandestins.

proposition de la Commission concernant une décision-cadre relative à la protection des données traitées dans le cadre du troisième pilier. La proposition d'origine a été examinée et révisée; le CEPD a suivi très attentivement l'évolution de cette question, rendant son troisième avis le 27 avril et envoyant une lettre à la présidence portugaise le 16 octobre (voir les points 3.3 et 3.4).

La conférence des autorités européennes chargées de la protection des données, qui s'est tenue à Lárnaka (Chypre) les 10 et 11 mai 2007, a adopté une déclaration dans la ligne de l'avis du CEPD. Ces autorités ont réaffirmé qu'il est essentiel de disposer d'un niveau élevé de protection des données, dans un cadre harmonisé couvrant les activités policières et judiciaires, lorsque l'on instaure un espace de liberté, de sécurité et de justice. Par ailleurs, elles ont déploré le fait que les négociations évoluaient dans le sens d'un champ d'application restreint et d'un niveau insatisfaisant de protection des données <sup>(67)</sup>.

La deuxième question concernait l'échange d'informations en matière répressive, conformément au principe de disponibilité, et notamment l'initiative de quinze États membres visant à rendre le traité de Prüm — fixant les modalités des échanges transfrontaliers de données biométriques dans le cadre de la lutte contre le terrorisme et la criminalité transfrontalière — applicable dans l'ensemble de l'UE. Le CEPD a rendu deux avis, le 4 avril 2007, sur l'initiative du traité de Prüm elle-même et, le 19 décembre 2007, sur ses modalités d'application (voir le point 3.3).

<sup>(67)</sup> Déclaration concernant le projet de décision-cadre relative à la protection des données dans le cadre du troisième pilier, adoptée le 11 mai 2007 et figurant sur le site internet du CEPD, onglet «Coopération», section «Conférence européenne».

Dans ce contexte, le CEPD a contribué à l'élaboration de la position commune des autorités européennes de protection des données sur le recours au concept de disponibilité en matière de répression, adoptée à Lárnaka par la conférence des autorités européennes chargées de la protection des données<sup>(68)</sup>. Cette déclaration, et la liste de contrôle y annexée, fournit des lignes directrices aux institutions européennes et aux parlements nationaux sur la manière de garantir que les instruments relatifs au principe de disponibilité permettent un gain d'efficacité en matière de répression, tout en assurant le respect du droit fondamental à la protection des données à caractère personnel.

La conférence de Lárnaka a aussi décidé de conférer un mandat élargi au groupe «Police», qui suit les questions liées au troisième pilier dans le cadre de la conférence. La nécessité croissante d'un contrôle permanent et d'une réaction rapide et efficace aux initiatives relevant du troisième pilier exige de mettre en place un forum plus stable et structuré. Dans le cadre de son mandat élargi, le groupe «Police et justice» (le nouveau nom du groupe) suivra notamment les évolutions observées dans le domaine répressif à l'égard du traitement des données à caractère personnel, préparera toutes les mesures que la conférence devra engager dans ce domaine et agira au nom de la conférence lorsqu'il sera impératif de réagir rapidement. Dans cette perspective, la conférence a nommé aux fonctions respectives de président et de vice-président du groupe, pour un mandat de deux ans, M. Francesco Pizzetti, président de l'autorité italienne de la protection des données, et M. Bart De Schutter, membre de l'autorité belge de la protection des données.

Le CEPD a activement contribué aux trois réunions que le groupe «Police et justice» a tenues en 2007. Après avoir adopté son règlement intérieur et défini ses méthodes de travail, le groupe a mené des travaux sur différents points importants:

- une lettre à la présidence portugaise concernant l'examen par le Conseil de la décision-cadre relative à la protection des données traitées dans le cadre du troisième pilier;
- une première discussion sur les modalités d'application de l'initiative Prüm;
- un avis sur la proposition de système PNR de l'UE, adopté conjointement avec le groupe de l'article 29;
- la nécessité d'une politique commune dans le domaine du contrôle des activités liées à la répression.

En outre, tant le CEPD que le président du groupe «Police et justice» ont participé à une réunion de la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (commission LIBE) sur la situation en matière de protection des données traitées dans le cadre du troisième pilier.

<sup>(68)</sup> Déclaration sur le principe de disponibilité, comportant la position commune et une liste de contrôle, adoptée le 11 mai 2007 et figurant sur le site internet du CEPD, onglet «Coopération», section «Conférence européenne».

## 4.5. Conférence européenne

Les autorités chargées de la protection des données des États membres de l'UE et du Conseil de l'Europe se rencontrent annuellement lors d'une conférence de printemps, pour discuter de questions d'intérêt commun ainsi que pour échanger des informations et partager leur expérience sur différents sujets. Le CEPD et le CEPD adjoint ont pris part à la conférence de Lárnaka, organisée les 10 et 11 mai 2007 par le commissaire à la protection des données à caractère personnel de Chypre.

Le CEPD a participé à la session consacrée à la protection des données dans les institutions de l'UE. La conférence a également porté sur d'autres points, à savoir: «dossiers médicaux électroniques», «protection des données, la voie à suivre», «protection des données traitées dans le cadre du troisième pilier», «les médias et la protection des données à caractère personnel», «les enfants et les données à caractère personnel» et d'autres questions actuelles. La conférence a également adopté un certain nombre de textes importants (voir le point 4.4).

La prochaine conférence européenne aura lieu à Rome, les 17 et 18 avril 2008, et fera le point sur les questions devant faire l'objet d'une attention particulière.

Des membres du personnel ont participé à des ateliers de traitement des dossiers, à Helsinki et à Lisbonne, en avril et en novembre 2007. Cet intéressant mécanisme de coopération au niveau du personnel — pour un échange de bonnes pratiques entre les autorités européennes chargées de la protection des données — est entré dans sa neuvième année. Le prochain atelier de traitement de dossiers aura lieu à Ljubljana en mars 2008.

## 4.6. Conférence internationale

Les autorités chargées de la protection des données et les commissaires à la protection de la vie privée d'Europe et d'autres parties du monde, notamment le Canada, l'Amérique latine, l'Australie, la Nouvelle-Zélande, Hong Kong, le Japon et d'autres territoires de la région Asie-Pacifique, se réunissent tous les ans à l'automne depuis plusieurs années. La 29<sup>e</sup> conférence internationale des commissaires à la protection des données et à la vie privée s'est tenue à Montréal du 25 au 28 septembre 2007 et a été organisée par la commissaire à la protection de la vie privée du Canada. Un grand nombre de délégués de quelque 60 pays du monde entier y ont participé.

Le thème de la conférence («Les horizons de la protection de la vie privée: terra incognita») était centré sur les nombreuses questions difficiles traitées par les commissaires à la protection des données et à la vie privée. Les principaux défis à relever, assimilés à des «dragons», concernaient les domaines suivants: la sécurité publique, la mondialisation, le droit et la technologie, l'informatique omniprésente, la prochaine

génération et le corps humain comme donnée. Certains ateliers ont examiné les moyens d'action possibles (les «pourfendeurs de dragons») tels que les analyses d'impact sur la vie privée, les audits et la sensibilisation des enfants à la vie privée.

Le CEPD et le Contrôleur adjoint de la protection des données ont tous deux participé à la conférence. Le CEPD a présidé une session, réservée aux commissaires, sur l'initiative de Londres (voir le point 4.7) et a contribué à un atelier sur la mondialisation.

La conférence a adopté trois résolutions <sup>(69)</sup> concernant:

- l'urgence d'établir des normes mondiales visant la protection des données des passagers dont se serviront les gouvernements pour appliquer les lois et assurer la sécurité frontalière;
- l'élaboration des normes internationales (appelant à une participation plus active aux mécanismes ISO);
- la coopération internationale (notamment l'application transfrontalière de la législation et les actions de sensibilisation à la protection des données).

La prochaine conférence internationale se déroulera à Strasbourg du 15 au 17 octobre 2008 et sera organisée conjointement par la Commission nationale de l'informatique et des libertés (CNIL), l'autorité française compétente en matière de protection des données, et le commissaire fédéral allemand à la protection des données et à la liberté de l'information.

#### 4.7. L'initiative de Londres

Une déclaration intitulée «Communiquer sur la protection des données et la rendre effective», qui a reçu le soutien général d'autorités de protection des données du monde entier, a été présentée lors de la 28<sup>e</sup> conférence internationale qui s'est déroulée à Londres en novembre 2006. Il s'agissait d'une initiative conjointe (appelée depuis «initiative de Londres») du président de l'autorité française de protection des données (la CNIL), du commissaire à l'information du Royaume-Uni (Information Commissioner) et du CEPD. En tant qu'un des principaux instigateurs de l'initiative de Londres, le CEPD est déterminé à contribuer activement au suivi des travaux avec les autorités nationales chargées de la protection des données <sup>(70)</sup>.

Dans le cadre de cette initiative, le président de la CNIL a organisé à Paris, en février 2007, un atelier sur les questions de communication. Ce dernier a débouché notamment sur la création d'un réseau d'agents de communication pour l'échange d'expérience et de bonnes pratiques dans leur domaine (voir aussi le point 5.1).

<sup>(69)</sup> Disponibles sur le site internet du CEPD, onglet «Coopération», section «Conférence internationale».

<sup>(70)</sup> Voir le rapport annuel de 2006, points 4.5 et 5.1.

Le CEPD a organisé à Bruxelles, en avril 2007, un atelier sur les questions d'application effective de la législation. Trois grands thèmes ont été examinés lors de cet atelier:

- les activités des autorités chargées de la protection des données, dans le domaine des inspections et des audits;
- une application renforcée au moyen d'interventions et de sanctions;
- les possibilités relatives au respect transfrontière de la législation.

Sur ce dernier thème, il a été tiré parti des travaux intéressants menés par l'Organisation de coopération et de développement économiques (OCDE). Il est apparu clairement que les autorités chargées de la protection des données sont de plus en plus actives dans le domaine de l'application effective de la législation. L'atelier a mis en évidence une expérience et des meilleures pratiques d'un très grand intérêt dans ce domaine.

Lors de la conférence internationale de Montréal (voir le point 4.6), le CEPD a présidé une session, réservée aux commissaires, sur l'initiative de Londres. Les possibilités d'actions futures ont été examinées tant pour l'UE que pour la région Asie-Pacifique, ce qui a mis en évidence la dimension réellement mondiale de cette initiative.

En décembre 2007, le commissaire à l'information du Royaume-Uni a organisé à Londres un atelier sur le thème des stratégies efficaces pour les autorités chargées de la protection des données. Il était axé sur des questions importantes en termes de planification stratégique et sur la manière de déterminer des priorités pour des actions efficaces («Sélectionner pour plus d'efficacité»).

Le CEPD se félicite que ces ateliers contribuent à rendre la protection des données plus efficace et à fournir des moyens pratiques d'atteindre cet objectif stratégique.

#### 4.8. Organisations internationales

Dans de nombreux cas, les organisations internationales ne sont pas soumises aux législations nationales. Il en résulte souvent une absence de cadre juridique pour la protection des données, même dans les cas où des données très sensibles sont collectées et échangées entre des organisations. La conférence internationale a évoqué cette question dans une résolution formulée en 2003 à Sydney et appelant «les organismes internationaux et supranationaux à s'engager formellement à respecter les principaux instruments internationaux en matière de protection des données et de la vie privée».

En collaboration avec le Conseil de l'Europe et l'OCDE, le CEPD a organisé, en septembre 2005, un séminaire sur la protection des données dans le cadre de la bonne gouvernance des organisations internationales. L'objectif était de sensibiliser les participants aux principes universels de la protection des données et à leurs conséquences pour le travail des orga-

nisations internationales. Les représentants d'une vingtaine d'organisations ont pris part aux discussions portant sur la protection des données à caractère personnel des membres du personnel ou d'autres personnes concernées. Le traitement des données sensibles relatives à la santé, au statut des réfugiés ou aux condamnations pénales y a aussi été abordé.

Le CEPD a contribué à un deuxième séminaire, organisé à Munich par l'Office européen des brevets en mars 2007.

Des représentants de diverses organisations internationales y ont débattu de sujets d'intérêt commun, comme le rôle des délégués à la protection des données, les moyens de mettre en place un régime de protection des données et la coopération internationale entre organismes qui ne suivent pas les mêmes normes en matière de protection des données.

Il est actuellement envisagé d'organiser un troisième atelier en 2008-2009.

## 5. Communication

### 5.1. Introduction

Les activités d'information et de communication continuent d'occuper une place importante dans la stratégie du CEPD et dans son travail quotidien. Bien qu'elles ne fassent pas partie de ses missions essentielles, abordées dans les chapitres précédents, on ne peut sous-estimer l'importance décisive que l'information et la communication revêtent en termes d'incidence concrète de ces missions. Cela se vérifie à différents niveaux. Il est essentiel que l'ensemble des parties concernées soient bien **sensibilisées à la protection des données** pour que les activités dans ce domaine se poursuivent de manière efficace. Les personnes concernées doivent connaître les droits spécifiques dont elles bénéficient avant de pouvoir les exercer de manière efficace. Les contrôleurs responsables doivent être au fait de leurs obligations avant de pouvoir faire respecter la législation. Les acteurs institutionnels doivent connaître l'incidence que leurs politiques pourraient avoir sur la protection des données à caractère personnel et savoir dans quels cas la protection des données peut contribuer à une plus grande légitimité et à de meilleurs résultats. Enfin, l'information et la communication sont également des outils essentiels pour assurer la transparence des politiques et des activités du CEPD.

Le CEPD a été l'un des principaux instigateurs de l'**initiative de Londres**, conçue pour rendre plus efficaces la communication sur la protection des données et la protection des données elle-même (voir aussi le point 4.7). Le CEPD en a assuré le suivi en février 2007 en participant activement à l'atelier de communication organisé par la CNIL, l'autorité française compétente en matière de protection des données. La création d'un **réseau d'agents de communication** (auquel contribue le CEPD) en a été un résultat important. Les autorités chargées de la protection des données pourront y faire appel afin d'échanger des bonnes pratiques et de réaliser des projets spécifiques tels que l'élaboration d'actions conjointes pour répondre à certains événements.

Un autre aspect essentiel de la sensibilisation à la protection des données réside dans la **coopération entre les délégués à la protection des données** dans les institutions et organes de l'Union européenne. Une coopération étroite entre les

DPD constitue un moyen ingénieux de partager les bonnes pratiques et de travailler efficacement ensemble afin de sensibiliser les acteurs et le personnel de l'UE aux questions de protection des données. Le CEPD souhaite vivement renforcer cette coopération entre les DPD en encourageant la mise en œuvre d'actions et d'initiatives communes, par exemple dans le cadre d'événements tels que la Journée de la protection des données. Travailler ensemble dans un cadre cohérent permet ainsi de maximiser l'impact des efforts de communication.

Ce chapitre présente les activités menées en 2007 par le CEPD dans le domaine de l'information et de la communication, qui englobent les travaux du service de presse, l'utilisation et la mise au point d'outils d'information en ligne (comme le site internet et le bulletin d'information), la participation à des ateliers et à des conférences, l'organisation d'entretiens, de visites et de conférences de presse, ainsi que les relations avec les médias (par la publication, par exemple, de matériel d'information et par des contacts réguliers avec les journalistes).

### 5.2. Caractéristiques de la communication

La politique de communication du CEPD doit être conçue en fonction de caractéristiques pertinentes au regard de la jeunesse, de la taille et du champ d'application de l'institution. Elle suit ainsi une stratégie sur mesure et a recours aux outils les plus appropriés pour cibler le public requis, tout en s'adaptant à un certain nombre de contraintes et d'exigences.

#### Public/groupes cibles

À la différence de la plupart des autres institutions et organes de l'Union européenne, dont les politiques et les activités de communication doivent être menées à un niveau général pour cibler l'ensemble des citoyens de l'Union, le champ d'action du CEPD est beaucoup plus spécifique. Il s'adresse avant tout aux institutions et organes de l'Union, aux per-

sonnes concernées en général et au personnel de l'UE en particulier, aux acteurs politiques de l'UE ainsi qu'aux «colègues de la protection des données». Il n'est donc pas nécessaire que la politique de communication du CEPD suive une stratégie de «communication de masse». Au contraire, la sensibilisation des citoyens de l'UE aux questions de protection des données, au niveau des États membres, dépend d'une approche plus indirecte, passant principalement par les autorités nationales chargées de la protection des données ainsi que par les centres d'information et les points de contact.

Le CEPD, toutefois, prend en charge la part qui lui incombe en vue de mieux se faire connaître du grand public, notamment grâce à un certain nombre d'outils de communication (site internet, newsletters et autres supports d'information), à des contacts réguliers avec les parties intéressées (accueil d'étudiants, par exemple) et à la participation à des événements publics, des réunions et des conférences.

### Langage utilisé

La politique de communication du CEPD doit aussi tenir compte de la nature relativement complexe de son champ d'activités.

Il est vrai que les questions de protection des données peuvent être considérées comme assez techniques et obscures pour les non-spécialistes, et le langage de communication doit être adapté en conséquence, notamment dans le cas d'outils d'information et de communication visant toutes sortes de public, tels que le site internet et les brochures d'information. Pour ces outils, de même que pour les réponses aux demandes d'informations émanant des citoyens, il convient de rédiger dans un style clair et intelligible qui évite tout jargon inutile.

Si le public visé est plus spécialisé (médias, experts de la protection des données, acteurs de l'UE, etc.), l'emploi de termes techniques et juridiques est plus justifié. Ainsi, une même information peut nécessiter d'être communiquée en utilisant un format et un style bien adaptés, en vue de refléter de manière appropriée le public visé (grand public/public plus spécialisé).

### Impact

Afin de maximiser l'impact obtenu, le style de communication du CEPD est guidé par le principe selon lequel «trop d'information tue l'information», rappelant ainsi qu'il convient d'éviter toute «surcommunication». Le recours aux outils de communication «traditionnels» (communiqués de presse, newsletters) est donc volontairement limité aux thèmes de grande portée, pour lesquels il est jugé à la fois nécessaire et opportun de réagir et d'informer le public le plus large possible.

### Visibilité

Au cours de ses premières années d'existence, le CEPD, en tant qu'institution récente, avait clairement pour objectif, dans le cadre de ses activités de communication, d'augmenter sa visibilité sur l'échiquier politique de l'Union européenne. Dans un délai relativement court, un travail important a pu être accompli en ce sens. Trois ans après le début des activités, les efforts consentis en matière de communication commencent à porter leurs fruits.

À titre d'exemple, le CEPD figurait parmi les 50 nominés au prix de l'**Européen de l'année 2007** de l'*European Voice*, dont le but est de distinguer des personnalités européennes marquantes qui ont eu un impact sur l'agenda de l'UE pendant l'année considérée. Peter Hustinx a été reconnu comme ayant «évolué vers un rôle plus proactif, n'hésitant pas à faire entendre sa voix, même dans des domaines sensibles comme la politique de sécurité» <sup>(71)</sup>. Cette reconnaissance met en évidence une meilleure sensibilisation aux actions et aux positions du CEPD sur des questions sensibles en matière de protection des données, qui figurent au rang des priorités politiques de l'UE.

De plus, l'augmentation du nombre de demandes d'informations et de conseils reçues quotidiennement par le service de presse du CEPD en 2007 (voir le point 5.5) renforce davantage le point de vue selon lequel ce dernier est devenu une référence dans le domaine de la protection des données.

### 5.3. Discours

Le CEPD a continué à consacrer une part importante de son temps et de ses efforts à l'explication de sa mission et à la sensibilisation à la protection des données en général, ainsi qu'à un certain nombre de questions particulières, et ce à l'occasion de discours et d'interventions similaires devant différentes institutions et dans divers États membres tout au long de l'année.

Il a fréquemment participé à la commission LIBE du Parlement européen ou à des événements connexes. Le 27 février, il a présenté son avis sur la proposition de décision du Conseil portant création de l'Office européen de police. Le 26 mars, il est intervenu lors d'un séminaire public sur les dossiers passagers (PNR), SWIFT, la sphère de sécurité (*Safe Harbor*) et la protection des données au niveau transatlantique. Le 27 mars, il a également participé à un séminaire sur les instructions consulaires communes et l'utilisation des éléments biométriques. Le 10 avril, il est intervenu lors d'une audience publique sur l'avenir d'Europol. Le 11 avril, il a présenté son avis sur une initiative en vue de l'adoption de la décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terro-

<sup>(71)</sup> Voir le magazine *Presenting the EV50 2007*, p. 45 ([http://www.ev50.org/prs/EV50\\_Magazine\\_2007-pages28-54.pdf](http://www.ev50.org/prs/EV50_Magazine_2007-pages28-54.pdf)).



M. Peter Hustinx présente un exposé à l'Association européenne de management et de marketing financiers.

risme et la criminalité transfrontière, sur la base du traité de Prüm. Le 7 mai, il s'est exprimé lors d'une audience publique sur la décision de Prüm. Le 8 mai, il a présenté son troisième avis sur la proposition de décision-cadre du Conseil relative à la protection des données traitées dans le cadre du troisième pilier. Le 14 mai, il a présenté son rapport annuel 2006. Le 21 novembre, il a commenté la stratégie générale du Conseil concernant la protection des données dans le cadre du troisième pilier. Le 11 septembre, le Contrôleur adjoint de la protection des données a présenté l'avis du CEPD sur les obligations alimentaires lors d'une audience commune des commissions LIBE et JURI et, le 8 octobre, a traité de la protection à plusieurs niveaux des droits fondamentaux au cours d'un séminaire public de la commission LIBE.

Le 16 janvier, le CEPD a présenté ses priorités en matière de consultation sur les nouvelles législations au groupe «Protection des données» du Conseil. Il s'est rendu à Berlin le 4 mai pour examiner avec la présidence allemande la protection des données traitées dans le cadre du premier et du troisième pilier. Cette discussion s'est poursuivie le 7 mai à Bruxelles, se limitant à la protection des données traitées dans le cadre du troisième pilier. Le 24 mai, le CEPD a présenté son rapport annuel 2006 au groupe «Protection des données» du Conseil. Le 4 septembre, il a prononcé un discours sur les questions éthiques liées à l'utilisation d'éléments biométriques lors d'un séminaire organisé à Lisbonne par le Comité stratégique sur l'immigration, les frontières et l'asile. Le 13 mars, le Contrôleur adjoint de la protection des données a présenté l'avis du CEPD concernant Europol au groupe «Europol» du Conseil.

Le CEPD est également intervenu auprès d'autres institutions et organes de l'UE. À l'occasion d'une réunion du secrétariat général et des directeurs généraux de la Commission européenne le 22 mars, le CEPD et le Contrôleur adjoint se sont exprimés sur la conformité au règlement (CE)

n° 45/2001. Le 26 avril, le CEPD est intervenu lors d'une réunion plénière de l'organe de contrôle commun d'Eurojust. Il a également parlé de la conformité au règlement (CE) n° 45/2001 au cours d'une réunion des chefs d'agence qui a eu lieu le 11 juin. Le 12 juillet, le CEPD et le Contrôleur adjoint se sont rendus auprès d'Eurojust pour un exposé sur les questions relatives au troisième pilier. Le 7 décembre, le CEPD s'est adressé au personnel du Médiateur européen à Strasbourg. Le 19 avril, le Contrôleur adjoint a fait une présentation sur la conservation des données médicales lors d'une réunion du collège des chefs d'administration et, le 24 avril, il a présenté les tâches et les compétences du CEPD au cours d'une réunion de l'assemblée des comités du personnel des agences de l'UE, à Torrejón (Espagne).

Au cours de l'année, le CEPD s'est également rendu dans un certain nombre d'États membres. Le 8 février, il a prononcé un discours au ministère néerlandais de la justice à La Haye. Il est ensuite intervenu, le 2 avril, lors d'un colloque sur les autorités indépendantes qui s'est déroulé à Athènes. Le 10 mai, il a pris la parole lors de la conférence de printemps des commissaires européens à la protection des données qui s'est tenue à Lárnaka. Le 15 mai, il a présenté un exposé au cours d'un séminaire sur les systèmes d'identification avancés, organisé à Bruxelles. Le 24 mai, il a prononcé un discours sur les points stratégiques de la protection des données lors de la conférence «European Data Protection Intensive» à Amsterdam. Le 7 juin, il est intervenu à l'occasion d'une conférence sur la conformité dans le domaine pharmaceutique, organisée à Bruxelles. Le 21 juin, il a présenté un exposé, devant le barreau d'Athènes, sur le rôle du CEPD. Il a également pris la parole lors d'une conférence sur l'identification par radiofréquence, à Berlin, le 26 juin.

Les 2 et 3 juillet, le CEPD a prononcé plusieurs discours au cours de la conférence sur l'économie et la protection de la vie privée, qui s'est tenue à Cambridge (Royaume-Uni). Le 6 juillet, il était également présent à l'Institute of European Affairs de Dublin. Le 13 juillet, il a participé à un séminaire sur la protection des données, organisé à Sofia dans le cadre d'un jumelage. Le 24 août, il prononçait un discours à l'occasion d'un séminaire sur la vie privée se déroulant à Cambridge (États-Unis). Le 6 septembre, il a présenté un exposé au forum britannique de la protection des données, à Londres. Le 14 septembre, il s'est exprimé lors d'un séminaire du Conseil de l'Europe sur la coopération judiciaire, qui s'est tenu à Strasbourg. Le 19 septembre, il a prononcé un discours lors d'une conférence sur les cartes de paiement, à Paris. Le 20 septembre, il a pris la parole lors d'un séminaire EurActiv à Bruxelles. Il est également intervenu le 27 septembre lors de la conférence internationale des commissaires à la protection des données et à la vie privée organisée à Montréal.

Le 2 octobre, il a prononcé un discours lors d'un séminaire du forum européen de la biométrie, à Bruxelles. Le 10 octobre, il a participé, à Bruxelles, à un panel de discussions CEPS-Google sur la vie privée en ligne. Le lendemain, il

était à Londres pour intervenir lors d'une conférence sur la conformité en matière de protection des données. Le 13 octobre, il a parlé du rôle des autorités chargées de la protection des données lors de la conférence internationale intitulée «Réinventer la protection des données», qui s'est tenue à Bruxelles. Le 22 octobre, il s'est adressé aux participants de la conférence intitulée «Le droit au respect de la vie privée dans la société de la surveillance» à Varsovie. Le 26 octobre, il s'est exprimé sur le système SIS II lors de la conférence des autorités suisses de la protection des données, organisée à Solothurn. Il s'est également rendu à Vilnius, le 13 novembre, pour prendre part à une conférence de l'autorité lituanienne chargée de la protection des données. Le 15 novembre, il est intervenu lors d'une conférence sur l'identification par radiofréquence, à Lisbonne. Enfin, il convient de mentionner sa participation au séminaire sur la sécurité des données organisé par l'Agence européenne chargée de la sécurité des réseaux et de l'information à Bruxelles, le 10 décembre.

Le Contrôleur adjoint de la protection des données a effectué des présentations similaires. Il était présent à Barcelone, pour une journée de la protection des données, où il a présenté les nouvelles propositions législatives qui ont vu le jour dans l'Union européenne. Le 16 février, il est intervenu lors d'un séminaire sur la mobilité, le contrôle et les nouvelles technologies, organisé par le CEPS (Centre for European Policy Studies) à Bruxelles. Le 22 mars, il a témoigné devant une sous-commission de la Chambre des lords sur les dossiers passagers (PNR) et le traité de Prüm. Le 1<sup>er</sup> juin, il a pris part à un atelier sur la vie privée et la lutte contre le terrorisme, organisé par le commissaire aux droits de l'homme du Conseil de l'Europe, à Strasbourg. Le 6 juillet, il est également intervenu au cours de la conférence annuelle du CEPS sur les questions de contrôle démocratique et de responsabilité judiciaire dans le domaine de la liberté, de la sécurité et de la justice. Du 12 au 14 septembre, il a présenté plusieurs exposés au cours d'un séminaire du Conseil de l'Europe sur la protection des données et la coopération judiciaire et, le 14 septembre, il a pris la parole à l'occasion de la conférence régionale européenne Unesco-Conseil de l'Europe sur l'éthique et les droits de l'homme dans la société de l'information. Le 5 octobre, à Madrid, il a présenté le projet de décision-cadre relative à la protection des données dans le cadre du troisième pilier. Le 10 octobre, il s'est exprimé lors de la neuvième réunion plénière du réseau de Lisbonne (formation des juges) du Conseil de l'Europe. Enfin, il a prononcé un discours sur la protection des données et l'accès du public aux documents, le 23 octobre à Bilbao.

#### 5.4. Service de presse

En raison de la mobilité du personnel, le service de presse a connu une certaine discontinuité en 2007, bien que des dispositions internes aient été prises pour assurer la poursuite des travaux en cours dans le domaine de la communication.

Une nouvelle attachée de presse a été recrutée en décembre 2007 afin d'assurer la stabilité et le développement professionnel des actions de communication et des activités liées à la presse.

Le service de presse est responsable de la communication externe avec les médias à travers des contacts réguliers avec les journalistes. Il est également chargé des demandes d'informations et de conseils, de la rédaction des communiqués de presse et des newsletters, ainsi que de l'organisation de conférences de presse et d'entretiens avec le CEPD ou le Contrôleur adjoint. Par ailleurs, l'attachée de presse dirige une équipe d'information de nature flexible qui participe aux événements et aux activités de promotion (Journée de la protection des données, journée portes ouvertes de l'UE, notamment — voir le point 5.8), ainsi qu'à la production de matériel d'information destiné au public et aux journalistes.

En 2007, le service de presse a publié 14 communiqués de presse — soit une moyenne d'un par mois sur l'ensemble de l'année. La plupart concernaient de nouveaux avis législatifs présentant un intérêt significatif pour le public. Parmi les thèmes abordés figuraient la proposition de décision-cadre relative à la protection des données traitées dans le cadre du troisième pilier, l'inspection et l'audit d'Eurodac, la mise en œuvre de la directive 95/46/CE relative à la protection des données, la proposition de règlement relatif aux transports routiers, le système d'identification par radiofréquence, les modalités d'application du traité de Prüm et la proposition concernant un système européen de dossiers passagers (données PNR).



L'équipe d'information discute de la production de matériel d'information.



MM. Peter Hustinx et Joaquín Bayo Delgado présentent leur rapport annuel pour 2006 au cours d'une conférence de presse.

Les communiqués de presse sont publiés sur le site internet du CEPD et diffusés à un réseau de journalistes et de parties intéressées qui est régulièrement mis à jour. Les informations fournies dans ces communiqués de presse font généralement l'objet d'une large couverture médiatique, car elles sont souvent reprises dans la presse tant générale que spécialisée, tout en étant également publiées sur des sites internet, institutionnels ou non, qui vont des institutions et organes de l'UE aux ONG, aux instituts universitaires et aux sociétés du secteur des technologies de l'information, entre autres.

Une conférence de presse a été organisée au début du mois de mai 2007 afin de présenter à la presse le rapport annuel 2006 du CEPD. Ce fut l'occasion de souligner que, après trois années d'existence, le CEPD avait étendu ses activités de contrôle et de consultation et que l'administration de l'UE était à présent invitée à démontrer qu'elle avait accompli des avancées substantielles en matière de respect des obligations liées à la protection des données.

## 5.5. Demandes d'informations ou de conseils

En 2007, le nombre de demandes d'informations ou de conseils est resté relativement stable par rapport à 2006 (160 demandes en 2007 contre 170 en 2006). Ces deman-

des émanent d'un large éventail de personnes et d'acteurs, qui vont des parties prenantes dont l'activité est liée à l'UE et /ou qui travaillent dans le domaine de la protection des données (cabinets juridiques, consultants, associations, universités, etc.) aux citoyens souhaitant obtenir plus d'informations sur des questions de vie privée ou qui demandent une assistance dans la résolution de questions ou problèmes auxquels ils sont confrontés dans la vie courante.

Une large majorité de ces demandes ont été classées en tant que «**demandes d'informations**» — une vaste catégorie qui englobe, entre autres, les questions générales sur les politiques et la législation de l'UE, mais aussi les questions plus précises ayant trait à la protection des données dans les États membres ainsi que dans l'administration de l'UE. À titre d'exemple, les demandes d'informations reçues en 2007 ont couvert des questions relatives à la sécurité liées aux données à caractère personnel, aux technologies dans le domaine de la biométrie, à la vie privée sur l'internet, au transfert de données à caractère personnel vers des pays tiers, à l'accès aux informations personnelles dans le cadre d'EPSO, ainsi qu'à la mise en œuvre de la directive 95/46/CE dans les États membres.

Les demandes qui vont au-delà de l'aspect «information» et qui exigent donc une analyse plus approfondie sont classées comme «**demandes de conseils**». En 2007, elles n'ont représenté qu'une faible minorité des demandes (moins de 5 %)

et sont généralement traitées par des gestionnaires de dossiers. Ce sont principalement les fonctionnaires traitant directement ou indirectement de la protection des données dans les institutions et agences de l'UE qui ont demandé conseil. Il va sans dire que les consultations plus importantes menées sur des mesures administratives (voir le point 2.7) appartiennent à une autre catégorie.

Les demandes de conseils reçues en 2007 concernaient notamment l'accès du public aux listes des candidats admissibles dans le cadre des procédures du Parlement européen, les conditions de nomination des délégués à la protection des données, ainsi que les règles à observer dans le domaine de la protection des données en ce qui concerne la publication sur un site internet de photos de participants à un événement.

Comme pour les années précédentes, la plupart des demandes ont été reçues en anglais et, dans une moindre mesure, en français. Le service de presse a pu ainsi répondre rapidement, dans le délai imparti de 15 jours ouvrables. Toutefois, pour un certain nombre de demandes formulées dans d'autres langues officielles de l'UE, il a fallu faire appel au service de traduction du Conseil. Dans ces cas, tant la demande que la réponse ont été traduites afin que le demandeur puisse recevoir les informations appropriées dans sa langue maternelle.

## 5.6. Outils d'information en ligne

### Évolution du site internet

Le site internet du CEPD reste son outil de communication et d'information le plus important. C'est aussi sur ce site que les visiteurs peuvent avoir accès à l'ensemble des différents documents élaborés dans le cadre des activités du CEPD (avis, commentaires, priorités de travail, publications, discours, communiqués de presse, newsletters, informations sur les événements, etc.).

Une nouvelle version du site internet du CEPD a été lancée en février 2007. Elle recourt à la technologie des systèmes de gestion des contenus internet qui a été conçue pour faciliter la gestion d'un grand nombre de documents.

La page d'accueil, disponible dans toutes les langues de l'Union, présente le CEPD et ses principales fonctions. Les autres pages du site sont actuellement disponibles en anglais et en français. Toutefois, de nombreux documents figurant sur le site sont fournis dans toutes les langues communautaires.

Le site est subdivisé en quatre rubriques.

- La première («Le CEPD») comporte des informations générales sur le CEPD et sur le Contrôleur adjoint, ainsi que sur leur mission, la législation de l'UE en matière de protection des données et les publications du CEPD,

notamment le rapport annuel, les actualités et les coordonnées de contact.

- Les autres rubriques reflètent la répartition des principales missions du CEPD. La rubrique «Supervision» fournit des informations et des documents relatifs au contrôle, par le CEPD, du traitement des données à caractère personnel par les administrations de l'UE. Y figurent, entre autres, un grand nombre d'avis rendus par le CEPD après avoir reçu notification, par les institutions, d'opérations de traitement présentant des risques spécifiques. La rubrique «Consultation» a trait au rôle de conseil du CEPD. Les avis sur la législation proposée sont publiés au Journal officiel et peuvent être consultés dans toutes les langues communautaires dans la sous-section «Avis». La rubrique «Coopération» reprend les travaux entrepris en étroite collaboration avec les autorités nationales chargées de la protection des données, principalement au niveau européen ou international.

D'autres fonctionnalités en ligne, comme le registre des notifications qui a été élaboré en 2007, seront accessibles au public en 2008. D'autres outils d'information, tels qu'un glossaire et une rubrique des questions les plus fréquemment posées (FAQ), sont aussi en préparation en vue de développer le site internet et de mieux répondre aux attentes des visiteurs.

Le service de presse du CEPD a continué de participer aux travaux du comité éditorial interinstitutionnel internet



Page d'accueil du nouveau site internet du CEPD.

(CEiii) afin de se tenir au courant des dernières évolutions en matière de technologie de l'internet.

### Newsletter

La newsletter du CEPD fournit des informations sur les activités récentes du CEPD telles que les avis rendus au sujet de propositions législatives de l'UE et les avis relatifs aux contrôles préalables, accompagnées d'explications et de précisions contextuelles appropriées. Les newsletters sont disponibles sur le site internet du CEPD, et une fonction d'abonnement automatique figure aussi sur la page concernée <sup>(72)</sup>.

Cinq numéros de la newsletter du CEPD ont été publiés en 2007, soit en moyenne un tous les deux mois. La newsletter est publiée en anglais et en français.

Le nombre d'abonnés est passé de quelque 460 personnes fin 2006 à un total de 635 personnes fin 2007. Parmi les abonnés figurent, entre autres, les membres du Parlement européen, le personnel de l'UE et celui des autorités nationales chargées de la protection des données, ainsi que des journalistes, des universitaires, des sociétés du secteur des télécommunications et des cabinets juridiques. Cette augmentation sensible et constante du nombre d'abonnés depuis la première newsletter a conduit à une réflexion sur l'opportunité de moderniser la publication, dont la conception et la présentation seraient notamment plus conviviales. Ces améliorations seront donc envisagées au cours de l'année 2008.

La newsletter reste un moyen efficace d'attirer l'attention sur les nouveautés du site internet et de mieux sensibiliser aux activités les plus récentes du CEPD, ce qui a pour effet d'accroître la visibilité du site et d'encourager les visites. La newsletter peut également contribuer efficacement à la constitution d'un réseau communautaire s'intéressant aux activités de protection des données au niveau de l'UE.

## 5.7. Contacts avec les médias et visites d'étude

Le CEPD s'est prêté à une vingtaine d'entretiens avec des journalistes de la presse écrite, de la radio et de la télévision ou des médias électroniques de différents États membres ou pays tiers; il a notamment accordé des entretiens au *Financial Times* et à *Associated Press*, ainsi qu'à la radio ou à la télévision autrichienne, danoise, néerlandaise, allemande, polonaise et britannique. Par ailleurs, des informations relatives aux activités du CEPD sont fréquemment apparues dans *European Voice*, *EU Reporter* et dans les publications internes de diverses institutions.

Dans le cadre des efforts consentis pour accroître encore sa visibilité et renforcer l'interaction avec le monde universitaire, le CEPD a accueilli des groupes d'étudiants spécialisés

<sup>(72)</sup> <http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/27>.

dans le domaine de la protection des données et/ou dans celui de la sécurité des technologies de l'information. En mai 2007, par exemple, il a reçu un groupe d'étudiants allemands avec lesquels il a examiné les questions liées à la protection des données dans une «société de la surveillance». Le CEPD et le Contrôleur adjoint ont aussi participé aux «European Youth Media Days» en juin 2007.

## 5.8. Événements promotionnels

Participer à des événements dans le cadre de l'UE constitue pour le CEPD une excellente occasion de mieux faire connaître les droits des personnes concernées et les obligations qui incombent aux institutions et organes de l'UE dans le domaine de la protection des données.

### Journée de la protection des données

Le CEPD, les institutions de l'UE et les autorités nationales chargées de la protection des données ont été invitées, en 2007, à notifier au Conseil de l'Europe les événements qu'ils prévoyaient d'organiser dans le cadre de la première Journée européenne de la protection des données.

Le 25 janvier 2007, le CEPD a tenu un stand d'information au Parlement européen puis, le 26 janvier, à la Commission européenne, afin de sensibiliser le personnel de l'UE au thème de la protection des données et aux activités du CEPD.

À cette occasion, le CEPD a fourni des informations sur différents aspects de la protection des données considérés comme critiques à ce moment, tels que les dossiers passagers (données PNR), SWIFT, le système d'information Schengen, le système d'information sur les visas, la conservation des données de télécommunications et la surveillance par des caméras. Une attention particulière a été accordée aux droits des personnes concernées.

Une affiche a été conçue pour illustrer les questions de protection des données évoquées ci-dessus. Les visiteurs intéressés par le stand du CEPD ont également été invités à participer à un quiz sur la protection des données dans les institutions et organes de l'UE. Les gagnants ont reçu un prix par tirage au sort (des clés USB «CEPD»).

C'est le Conseil de l'Europe qui, avec le soutien de la Commission, a lancé la première célébration de la Journée de la protection des données le 28 juin 2007 — date qui tombait malheureusement un dimanche cette année-là. Cette date marque l'anniversaire de l'ouverture à la signature de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, en 1981. La convention a constitué le premier instrument international juridiquement contraignant dans le domaine de la protection des données.



Le stand du CEPD à la Commission européenne lors de la Journée de la protection des données, le 25 janvier 2007.



L'équipe chargée de tenir le stand du CEPD au Parlement européen lors de la journée portes ouvertes de l'UE, le 5 mai 2007.

### **Journée portes ouvertes de l'UE**

Le 5 mai 2007, le CEPD a participé à la journée portes ouvertes de l'UE organisée à Bruxelles par les institutions et organes de l'UE pour célébrer le Jour de l'Europe (le 9 mai).

Le CEPD a tenu un stand dans les locaux du Parlement européen, et des membres du personnel étaient présents pour répondre aux questions des visiteurs.

Différents supports d'information présentant les travaux du CEPD ont été distribués aux visiteurs, ainsi qu'une série d'objets promotionnels (stylos, autocollants, tasses et clés USB arborant le logo du CEPD). Les visiteurs ont également eu l'occasion de tester leurs connaissances dans le domaine de la protection des données en répondant à un quiz rapide et ont pu prendre part à un tirage au sort.

## 6. Administration, budget et personnel

### 6.1. Introduction: développement de la nouvelle institution

Le développement du CEPD en tant que nouvelle institution <sup>(73)</sup> s'est poursuivi en vue de consolider les bonnes bases sur lesquelles il a commencé à fonctionner. En 2007, le CEPD a pu disposer de **ressources supplémentaires** tant au niveau de son budget (qui est passé de 4 138 378 euros à 4 955 726) qu'à celui de son personnel (24 personnes en 2006, 29 en 2007).

Le développement de l'**environnement administratif** se poursuit progressivement en fonction des priorités annuelles, compte tenu des besoins et de la taille de l'institution. Le CEPD a adopté différentes règles internes <sup>(74)</sup> nécessaires au bon fonctionnement de l'institution. Le comité du personnel est étroitement associé aux travaux portant sur les dispositions générales d'application du statut et d'autres règles internes adoptées par l'institution. L'auditeur interne a communiqué les conclusions du premier audit interne en 2007.

La coopération avec d'autres institutions (Parlement européen, Conseil et Commission européenne) s'est encore améliorée, ce qui a permis de réaliser des économies d'échelle considérables. Le problème du ralentissement de certaines tâches, dans le cadre de l'assistance partagée (ce qui concerne principalement l'accès aux logiciels administratifs et financiers), a été en partie résolu. Le CEPD a pris en charge certaines tâches qui étaient initialement accomplies par d'autres institutions.

<sup>(73)</sup> L'article 1<sup>er</sup> ter du statut des fonctionnaires des Communautés européennes et l'article 1<sup>er</sup> du règlement financier prévoient que, aux fins desdits règlements, le CEPD est assimilé à une institution des Communautés. Voir aussi l'article 43, paragraphe 6, du règlement (CE) n° 45/2001.

<sup>(74)</sup> Une liste des accords et décisions de nature administrative figure à l'annexe I.



Unité «Personnel, budget et administration».

### 6.2. Budget

Le budget adopté par l'autorité budgétaire pour l'exercice 2007 s'élevait à 4 955 726 euros, ce qui représente une augmentation de 19,8 % par rapport au budget 2006.

En 2007, le CEPD a adopté une nouvelle terminologie budgétaire, qui s'appliquera à l'établissement du budget 2008. Elle se fonde sur les trois années d'expérience du CEPD, en tenant compte des besoins spécifiques de l'institution et en veillant à la transparence requise par l'autorité budgétaire.

Le CEPD applique les règles internes de la Commission sur l'exécution du budget, dans la mesure où celles-ci sont applicables à la structure de son budget et à la taille de l'organisation et compte tenu de l'absence de règles spécifiques.

La Commission a continué de fournir une assistance, en particulier dans le domaine de la comptabilité, le comptable de la Commission ayant également été désigné comptable du CEPD. Pour ce qui est des logiciels financiers, le CEPD

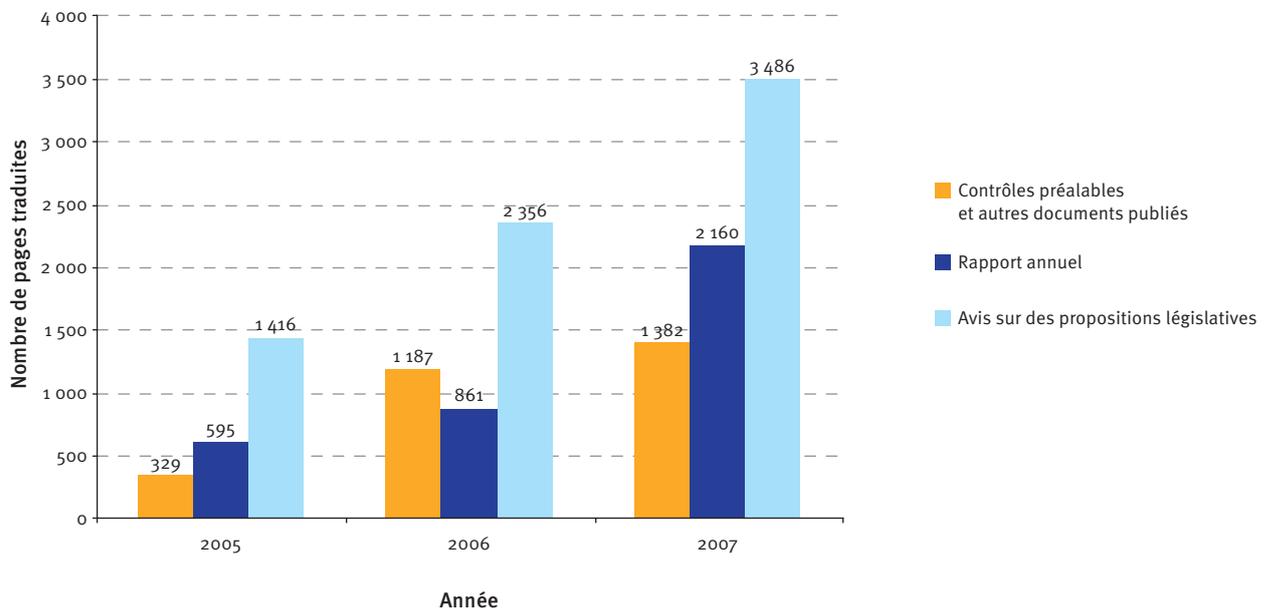


Tableau 1. Évolution du volume des traductions

a obtenu un accès direct à un programme (intitulé «ABAC Workflow»), grâce auquel les transactions financières peuvent être traitées dans les locaux de l'institution.

Dans son rapport concernant l'exercice 2006, la Cour des comptes européenne a indiqué que l'audit n'avait donné lieu à aucune observation.

Une part importante du budget est consacrée aux traductions, qui ont une incidence non négligeable sur les travaux administratifs. Les avis du CEPD relatifs aux propositions législatives sont traduits dans 22 langues officielles de l'Union européenne, à l'exception, provisoirement, de l'irlandais. Ils sont publiés au *Journal officiel de l'Union européenne*. En 2007, le CEPD a rendu 12 avis. Depuis 2005, une augmentation constante du nombre d'avis et du nombre de langues officielles a pu être observée. De ce fait, le nombre de pages à traduire a plus que doublé.

Les avis sur les contrôles préalables et d'autres documents publiés sont en général uniquement traduits dans les langues de travail des institutions européennes. En 2007, le CEPD a produit 151 documents officiels devant être traduits. Cette catégorie de documents a plus que triplé depuis 2005.

Le nombre de missions effectuées par les membres et le personnel du CEPD a doublé depuis 2005, ce qui est la conséquence logique de l'accroissement des activités de l'institution. L'équipe administrative gère les aspects financiers des missions avec l'aide du PMO.

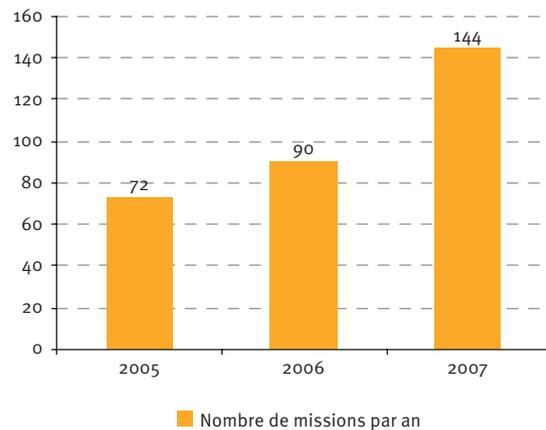


Tableau 2. Évolution du nombre de missions

### 6.3. Ressources humaines

Le CEPD bénéficie de l'aide efficace des services de la Commission en ce qui concerne les tâches liées à la gestion du personnel de l'institution (à savoir les deux membres nommés et les vingt-neuf membres du personnel).

#### 6.3.1. Recrutement

En tant qu'institution récemment créée, le CEPD en est encore au stade de la mise en place, ce qui sera le cas pour quelques années encore. La visibilité croissante de l'institution se traduit par une augmentation de la charge de travail, qui s'accompagne d'un accroissement du nombre de ses tâches. L'augmentation sensible de la charge de travail en 2007 a été décrite dans les chapitres précédents. Les ressources humaines ont bien évidemment un rôle fondamental à jouer dans ce cadre.

Le choix du CEPD est néanmoins de limiter cet accroissement des tâches et du personnel par une progression contrôlée afin d'assurer la pleine intégration ainsi qu'une insertion et une formation satisfaisantes des nouveaux collègues. Le CEPD a donc demandé la création de cinq postes seulement en 2007 (quatre administrateurs et un assistant). L'autorité budgétaire ayant accédé à cette demande, le tableau des effectifs est passé de vingt-quatre personnes en 2006 à vingt-neuf en 2007. Les avis de vacance ont été publiés au début de l'année 2007, et tous les postes ont été pourvus au cours de l'année.

La Commission, et plus particulièrement le PMO et le service médical, ont fourni une aide précieuse.

Le CEPD a accès aux services offerts par EPSO et participe aux travaux de son conseil d'administration, pour le moment en tant qu'observateur.

#### 6.3.2. Programme de stages

Un programme de stages a été créé en 2005. Son principal objectif est d'offrir aux jeunes diplômés des universités la possibilité de mettre en pratique les connaissances acquises durant leurs études, et d'acquérir ainsi une expérience pratique en participant aux activités quotidiennes du CEPD. Ce dernier a ainsi l'occasion d'accroître sa visibilité auprès des jeunes citoyens de l'UE, en particulier auprès des étudiants des universités et des jeunes diplômés spécialisés dans la protection des données.

Le programme principal accueille en moyenne deux stagiaires par session; deux sessions de cinq mois sont organisées chaque année, de mars à juillet et d'octobre à février. Les résultats ont été particulièrement positifs.

Outre le programme de stages principal, des dispositions spéciales ont été prévues pour accepter des étudiants des universités et des étudiants en doctorat pour des stages de courte durée non rémunérés. La seconde partie du programme donne aux jeunes étudiants la possibilité de mener des recherches dans le cadre de leur thèse. Cette activité se

déroule conformément au processus de Bologne et répond à l'obligation faite aux étudiants d'effectuer un stage dans le cadre de leurs études. À la fin de l'année 2007, un étudiant en doctorat a été sélectionné pour un stage de deux mois non rémunéré. Ces stages sont limités à des situations exceptionnelles et soumis à des critères d'admission très stricts.

Tous les stagiaires, rémunérés ou non, ont contribué à la fois au travail théorique et pratique, tout en acquérant une expérience directe.

Sur la base d'un accord au niveau des services signé en 2005, le CEPD a bénéficié d'une assistance administrative de la part du bureau des stages de la direction générale de l'éducation et de la culture de la Commission, qui a continué à apporter un soutien précieux grâce à l'expérience considérable de son personnel.

#### 6.3.3. Programme pour les experts nationaux détachés

Le programme destiné aux experts nationaux détachés (END) a été lancé en janvier 2006, à la suite de la mise en place de sa base juridique et organisationnelle à l'automne 2005 <sup>(75)</sup>.

Le détachement d'experts nationaux permet au CEPD de bénéficier des compétences et de l'expérience professionnelle de membres des autorités de protection des données des États membres. Ce programme permet aux experts nationaux de se familiariser avec les questions de protection des données dans le cadre de l'UE (en termes de contrôle, de consultation et de coopération). Le bénéfice est réciproque dans la mesure où le programme permet aussi au CEPD d'accroître sa visibilité, au niveau national, dans le domaine de la protection des données.

Afin de recruter des experts nationaux, le CEPD s'adresse directement aux autorités nationales chargées de la protection des données. Les représentations permanentes nationales sont également informées du programme et sont invitées à participer à la recherche de candidats correspondant au profil recherché. La DG Personnel et administration de la Commission fournit une aide administrative précieuse à l'organisation de ce programme.

En 2007, deux experts nationaux ont été détachés, l'un de l'autorité britannique chargée de la protection des données — le bureau du commissaire à l'information — et l'autre de l'autorité hongroise chargée de la protection des données — le commissaire à la protection des données et à la liberté de l'information.

#### 6.3.4. Organigramme

L'organigramme du CEPD est resté le même depuis 2004: une unité, composée à présent de huit personnes, est chargée

<sup>(75)</sup> Décision du CEPD du 10 novembre 2005.

de l'administration, du personnel et du budget; les 21 autres membres du personnel sont chargés de l'aspect opérationnel des tâches de protection des données. Ils travaillent directement sous l'autorité du CEPD et du Contrôleur adjoint dans deux grands domaines ayant trait au contrôle et à la consultation.

Une certaine souplesse a néanmoins été maintenue dans l'attribution des tâches du personnel, étant donné que les activités de l'institution sont encore en évolution.

### 6.3.5. Formation

Un objectif fondamental de la formation du personnel du CEPD est d'élargir et d'améliorer les compétences personnelles afin que chaque membre du personnel puisse contribuer avec la plus grande efficacité à la réalisation des objectifs de l'institution. En 2007, le CEPD a adopté une **politique de formation interne** fondée sur les activités spécifiques de l'institution, ainsi que sur ses objectifs stratégiques. Les orientations générales, figurant en annexe à la décision correspondante, définissent les domaines d'apprentissage prioritaires pour la période 2007-2008. L'objectif est d'élaborer un «centre d'excellence» dans le domaine de la protection des données et d'améliorer les connaissances et les compétences du personnel de façon qu'il fasse siennes les valeurs du CEPD.

Une journée d'accueil a été organisée à l'attention des nouveaux collègues. Elle repose sur un programme standard qui leur donne une idée générale de l'institution et de l'environnement administratif.

Le personnel du CEPD a accès aux cours de formation organisés par d'autres institutions européennes et organes interinstitutionnels, à savoir principalement la Commission et l'École européenne d'administration (EEA).

Pour le CEPD, participer aux groupes de travail interinstitutionnels (le groupe de travail interinstitutionnel de l'EEA et le comité interinstitutionnel de la formation linguistique) permet de partager une approche commune dans un secteur où les besoins des différentes institutions sont, pour l'essentiel similaires, et de réaliser des économies d'échelle.

En 2007, le CEPD a signé, avec les autres institutions, un nouveau protocole sur l'harmonisation des dépenses liées aux cours de langues interinstitutionnels.

## 6.4. Assistance administrative et coopération interinstitutionnelle

La coopération interinstitutionnelle, qui est fondée sur l'accord de coopération interinstitutionnelle signé en juin 2004 et prolongé pour une période de trois ans en 2006, demeure essentielle pour le CEPD et ses activités, en termes d'accroissement de l'efficacité et d'économies d'échelle. Elle permet également d'éviter la multiplication des infrastructures admi-

nistratives et de réduire les dépenses administratives improductives, tout en garantissant un niveau élevé de gestion des services publics.

En 2007, la coopération interinstitutionnelle s'est poursuivie sur cette base avec diverses directions générales de la Commission (DG Personnel et administration; DG Budget; service d'audit interne; DG Éducation et culture), l'Office des paiements (PMO), différents services du Parlement européen (services de l'information et des technologies, en ce qui concerne plus particulièrement la mise en place de la nouvelle version du site internet du CEPD; équipement des locaux; sécurité des bâtiments; travaux d'impression; courrier; téléphonie; fournitures; etc.) et le Conseil (pour ce qui est des traductions).

Les accords au niveau des services qui ont été signés en 2005 avec les diverses institutions et leurs services sont régulièrement mis à jour. Des accords couvrant de nouveaux domaines sont en cours de préparation.

Afin de faciliter la coopération entre les services de la Commission et le CEPD et d'améliorer l'échange d'informations entre les services, il a été demandé en 2006 que le CEPD puisse disposer d'un accès direct à certaines applications de gestion financière de la Commission (ABAC, SAP). Cet accès direct a été mis en place pour le système ABAC et se trouve en cours de développement pour l'application SAP. En ce qui concerne les applications de gestion des ressources humaines, le CEPD ne dispose toujours que d'un accès partiel au système Syslog<sup>(76)</sup>. Un accès sans restriction devrait être possible au cours de l'année 2008.

La refonte du site internet du CEPD a été réalisée en coopération avec les services compétents du Parlement européen. Toutefois, des problèmes liés au logiciel qui avait été spécifiquement choisi pour cette tâche ont ralenti la finalisation du projet. Le CEPD espère qu'il pourra être terminé au cours de l'année 2008.

La participation à l'appel d'offres interinstitutionnel pour les agents intérimaires, les assurances et le mobilier s'est poursuivie en 2007, ce qui a permis à l'institution d'accroître son efficacité dans de nombreux domaines administratifs et d'avancer vers une plus grande autonomie. Pour ce qui est des fournitures de bureau, le CEPD a participé à l'appel d'offres du Parlement, ce qui aboutira à la conclusion de nouveaux contrats à l'été 2008.

Le CEPD a continué de participer à divers comités interinstitutionnels mais a dû se limiter à certains d'entre eux en raison de la taille réduite de l'institution. Cette participation a contribué à accroître la visibilité du CEPD auprès des autres institutions et favorisé l'échange continu d'informations et de bonnes pratiques.

<sup>(76)</sup> Syslog est un système d'information pour la gestion électronique des cours de formation. ABAC et SAP sont des systèmes de gestion de la comptabilité.

## 6.5. Infrastructure

Sur la base de l'accord de coopération administrative, le CEPD est situé dans les locaux du Parlement européen qui l'assiste dans les domaines des technologies de l'information (TI) et de l'infrastructure de téléphone.

L'inventaire du mobilier et des biens de TI a été réalisé avec l'aide des services du Parlement.

## 6.6. Environnement administratif

### 6.6.1. Systèmes de contrôle et d'audit internes

Le processus consistant à identifier les risques liés au développement des activités du CEPD en est encore clairement à ses débuts. Le CEPD a adopté les procédures spécifiques de contrôle interne jugées les mieux adaptées à ses besoins en fonction de la taille de l'institution et de ses activités. L'objectif est de fournir à la direction et au personnel une assurance raisonnable quant à la réalisation des objectifs de l'institution et à la gestion des risques liés à ses activités.

D'une manière générale, le CEPD estime que les systèmes de contrôle interne en place fournissent une assurance raisonnable sur la légalité et la régularité des opérations dont l'institution est responsable. Le CEPD veillera à ce que l'ordonnateur délégué poursuive ses efforts visant à garantir que l'assurance raisonnable des déclarations accompagnant les rapports annuels soit effectivement étayée par des systèmes de contrôle interne appropriés.

La première évaluation effectuée par les services du CEPD a démontré la fonctionnalité et l'efficacité du système de contrôle interne.

Le premier rapport d'audit réalisé par le service d'audit interne (SAI) a été reçu en septembre 2007. Il a confirmé que le système de contrôle interne du CEPD est capable de fournir une assurance raisonnable pour la réalisation des objectifs de l'institution. Ce processus d'évaluation a toutefois permis d'identifier certains aspects qu'il faut améliorer. Pour certains de ceux-ci, des mesures rapides ont été prises, tandis que d'autres seront progressivement mises en place, parallèlement à l'évolution des tâches confiées au CEPD.

La mise en œuvre des recommandations du SAI, sur lesquelles le CEPD a marqué son accord, a été définie comme priorité pour 2008. Elle sera entreprise sur la base d'un plan d'action qui sera élaboré au début de 2008.

Le CEPD a l'intention de progresser dans ce domaine en vue de maintenir au minimum le niveau de risque pour l'institution.

### 6.6.2. Comité du personnel

Conformément à l'article 9 du statut des fonctionnaires des Communautés européennes, le CEPD a adopté le 8 février 2006 une décision instituant un comité du personnel. Le comité est consulté sur une série de dispositions générales d'application du statut et sur d'autres règles internes adoptées par l'institution.

### 6.6.3. Règlement intérieur

Le processus d'adoption de nouvelles règles internes nécessaires au bon fonctionnement de l'institution s'est poursuivi ainsi que l'adoption de nouvelles dispositions générales d'application du statut (voir l'annexe I).

Lorsque ces dispositions concernent des domaines pour lesquels le CEPD bénéficie de l'assistance de la Commission, elles sont semblables à celles de la Commission, moyennant quelques adaptations liées à la spécificité des services du CEPD. Lors de leur premier jour, les collègues nouvellement recrutés reçoivent un guide administratif, qui comprend toutes les règles internes du CEPD et les informe des spécificités de l'institution. Ce document est régulièrement mis à jour.

Le CEPD a continué de développer des infrastructures sociales (principalement relatives aux enfants, telles que l'accès aux crèches, à l'École européenne, etc.).

Deux importantes décisions internes ont été adoptées en 2007:

- À la suite d'une étude approfondie des systèmes d'évaluation des autres institutions européennes et d'un dialogue productif avec le comité du personnel, le CEPD a adopté la décision n° 30 du 30 mars 2007 établissant des règles pour la **notation** de son personnel, conformément au statut des fonctionnaires des Communautés européennes <sup>(77)</sup>. Un guide destiné à la notation du personnel a été élaboré en vue de définir des critères d'évaluation et les modalités de l'exercice de notation. Un entretien à mi-parcours a été instauré, permettant de dialoguer avec le fonctionnaire noté après six mois, ce qui lui donne la possibilité d'améliorer ses performances bien avant la notation officielle. À la suite de l'adoption de ces règles, le premier exercice de notation a été réalisé en 2007.
- Le système de notation étant en place, la mise en œuvre d'un système de **promotion** était l'étape suivante logique dans le processus visant à créer et à perfectionner un environnement administratif et une structure de carrière. Le CEPD a adopté des règles régissant le système de promotion par la décision n° 38 du 26 novembre 2007. À la suite de l'adoption de cette décision, le premier exercice de promotion a pu être mené.

<sup>(77)</sup> En vertu de l'article 43: «La compétence, le rendement et la conduite dans le service de chaque fonctionnaire font l'objet d'un rapport périodique [...]»

Le CEPD est une institution relativement neuve et a connu une évolution rapide. En conséquence, les règles et procédures adoptées au cours des premières années d'activité pourraient se révéler moins efficaces à l'avenir, dans le cadre d'une structure plus importante et plus complexe. Pour ce motif, ces règles (par exemple, notation et promotion) feront l'objet d'une analyse deux ans après leur adoption et pourront être modifiées en conséquence.

En outre, un paquet de trois décisions relatives aux **droits à pension** du personnel a été adopté. Le CEPD a ouvert les négociations avec le PMO pour déléguer les activités quotidiennes dans ce domaine hautement technique.

#### 6.6.4. Délégué à la protection des données

En vertu de l'article 24, paragraphe 1, du règlement (CE) n° 45/2001, le CEPD a nommé un délégué à la protection des données pour assurer l'application interne des dispositions du règlement. Un inventaire des opérations de traitement de données à caractère personnel a été dressé en 2007. Cet inventaire vise à orienter le processus de notification. En raison de sa position spécifique, le CEPD élabore actuellement un processus de notification simplifié pour les cas soumis au contrôle préalable.

#### 6.6.5. Gestion des documents

Le CEPD a commencé à travailler sur la mise en œuvre d'un nouveau système de gestion du courrier électronique (GEDA) avec le soutien des services du Parlement européen. Il est prévu que ce soit la première étape dans la mise en place d'un système de gestion des dossiers pour mieux soutenir les activités du CEPD.

### 6.7. Relations extérieures

En tant qu'autorité européenne sise à Bruxelles et reconnue par les autorités belges, le CEPD ainsi que son personnel bénéficient des privilèges et immunités prévus par le protocole sur les privilèges et immunités des Communautés européennes.

### 6.8. Objectifs pour 2008

Les objectifs fixés pour 2007 ont été pleinement atteints. En 2008, le CEPD poursuivra le processus de consolidation engagé auparavant et développera davantage certaines activités.

La nouvelle terminologie **budgétaire** est applicable en 2008. Le CEPD prévoit l'adoption de nouvelles règles financières internes adaptées à la taille de l'institution. Il est prévu d'optimiser plusieurs processus de traitement interne afin que



Le comité du personnel du CEPD en réunion.

l'institution reste adaptée à la quantité toujours croissante de dossiers financiers à traiter. Pour ce qui est des logiciels financiers, le CEPD poursuivra ses efforts pour acquérir les outils permettant l'accès aux dossiers financiers depuis ses locaux.

La poursuite de la **coopération administrative** sur la base de l'accord administratif prorogé restera un facteur essentiel du développement du CEPD. Parallèlement, le CEPD continuera à développer l'environnement administratif de ses services et à adopter des dispositions générales d'application du statut.

Le système de traitement du courrier et de suivi des dossiers sera développé et amélioré grâce à l'aide des services du Parlement européen. Pour ce qui est des logiciels de gestion des ressources humaines [principalement MIP (missions) et Syslog (congés et formations)], le CEPD fera tous les efforts nécessaires pour acquérir les programmes permettant l'accès aux dossiers depuis ses locaux.

La mise en œuvre des améliorations identifiées au cours de la première évaluation du système de contrôle interne ainsi que la mise en œuvre des recommandations du service d'audit interne reçues à la fin de 2007 seront des priorités. Le CEPD continuera à assurer l'application interne des dispositions du règlement (CE) n° 45/2001.

Conscient du niveau de confidentialité requis par certains domaines de ses activités, le CEPD envisage d'élaborer une politique globale de **sécurité** compatible avec ses fonctions.

Des **espaces de bureaux** supplémentaires seront nécessaires pour accueillir le personnel futur. Des négociations en vue d'obtenir assez d'espace pour couvrir les besoins futurs seront engagées avec les services du Parlement européen au cours de l'année 2008.

Le CEPD a l'intention de développer ses activités en matière sociale et de mettre au point le développement du nouveau site internet.



## Annexe A

## Cadre juridique

L'article 286 du traité CE, adopté en 1997 dans le cadre du traité d'Amsterdam, dispose que les actes communautaires relatifs à la protection de personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes communautaires et qu'un organe indépendant de contrôle doit être institué.

Les actes communautaires visés dans cette disposition sont la directive 95/46/CE, qui définit le cadre général de la législation en matière de protection des données dans les États membres, et la directive 97/66/CE, qui a depuis été remplacée par la directive 2002/58/CE sur la vie privée et les communications électroniques. Ces deux directives peuvent être considérées comme le résultat d'une évolution du cadre juridique amorcée au début des années 70 au sein du Conseil de l'Europe.

## Contexte

L'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) consacre le droit au respect de la vie privée et familiale et définit les conditions dans lesquelles ce droit peut faire l'objet de restrictions. Cependant, en 1981, il a été considéré nécessaire d'adopter une convention distincte en matière de protection des données, afin de développer une approche positive et structurelle de la protection des droits fondamentaux et des libertés fondamentales, qui peut être affectée par le traitement des données à caractère personnel dans une société moderne. Cette convention, également appelée «convention 108», a été ratifiée par près de quarante pays membres du Conseil de l'Europe, dont l'ensemble des États membres de l'UE.

La directive 95/46/CE a repris les principes de la convention 108, en les précisant et en les développant de diverses manières. L'objectif était d'assurer un niveau élevé de protection et de permettre la libre circulation des données à caractère personnel au sein de l'UE. Quand la Commission a présenté la proposition de directive au début des années 90, elle a indiqué qu'il faudrait prévoir pour les institutions et organes communautaires des garanties juridiques similaires, afin de leur permettre de participer à la libre circulation des données à caractère personnel moyennant des règles de protection équivalentes. Mais jusqu'à l'adoption de l'article 286 du traité CE, il n'existait pas de base juridique pour un tel instrument.

Les dispositions utiles visées à l'article 286 du traité CE ont été prises dans le règlement (CE) n° 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, qui est entré en vigueur en 2001 <sup>(78)</sup>. Ce règlement a également institué, comme le prévoyait le traité, une autorité de contrôle indépendante, nommée le «Contrôleur européen de la protection des données», auquel un certain nombre de tâches et de compétences ont été assignées.

Le traité de Lisbonne, signé en décembre 2007, renforce la protection des droits fondamentaux de différentes manières. Le respect de la vie privée et familiale et la protection des données à caractère personnel sont traités comme des droits fondamentaux distincts dans les articles 7 et 8 de la charte des droits fondamentaux de l'UE, qui est devenue juridiquement contraignante. La protection des données est également traitée, par une disposition générale à l'article 16 du traité sur le fonctionnement de l'UE. Il est ainsi manifeste que la protection des données est désormais considérée comme un élément fondamental d'une bonne gestion des affaires publiques. Le contrôle indépendant est un élément essentiel de cette protection.

## Règlement (CE) n° 45/2001

En examinant de plus près le règlement, il convient de noter dans un premier temps qu'il s'applique au «traitement de données à caractère personnel par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire». Cela signifie que seules les activités qui sont totalement en dehors du premier pilier ne relèvent pas des tâches et des compétences de contrôle du CEPD.

Les définitions et la teneur du règlement s'inspirent très largement des principes de la directive 95/46/CE. On pourrait dire que le règlement (CE) n° 45/2001 constitue la mise en œuvre de cette directive au niveau des institutions européennes. Le règlement traite des principes généraux tels que le traitement loyal et licite, la proportionnalité et la compatibilité d'utilisation, les catégories particulières des données sensibles, l'information de la personne concernée, les droits de la personne concernée, les obli-

<sup>(78)</sup> JO L 8 du 12.1.2001, p. 1.

gations des responsables du traitement (en tenant compte, le cas échéant, des circonstances propres au niveau de l'UE) ainsi que du contrôle, de l'exécution et des recours. Un chapitre particulier est consacré à la protection des données à caractère personnel et de la vie privée dans le cadre des réseaux internes de télécommunications. Ce chapitre constitue en fait la mise en œuvre au niveau européen de la directive 97/66/CE sur la vie privée et les communications électroniques.

Une des caractéristiques intéressantes du règlement est l'obligation qui est faite aux institutions et organes communautaires de désigner au moins une personne comme DPD. Ces délégués sont chargés d'assurer, d'une manière indépendante, l'application interne des dispositions du règlement, y compris la notification appropriée des opérations de traitement. Des délégués sont désormais en place dans toutes les institutions communautaires et dans un certain nombre d'organes, pour certains depuis plusieurs années. Des travaux importants ont donc été accomplis pour mettre en œuvre le règlement, même en l'absence d'un organe de contrôle. Ces délégués peuvent d'ailleurs être mieux placés pour fournir des conseils ou intervenir à un stade précoce et pour contribuer à la mise au point de bonnes pratiques. Les délégués à la protection des données ayant l'obligation formelle de coopérer avec le CEPD, il s'est formé un réseau très important et fort apprécié, qu'il convient de développer encore (voir le point 2.2).

### Tâches et compétences du CEPD

Les tâches et les compétences du Contrôleur européen de la protection des données sont clairement énoncées aux articles 41, 46 et 47 du règlement (voir l'annexe B), à la fois en termes généraux et spécifiques. L'article 41 définit la mission principale du CEPD, qui consiste à veiller à ce que les libertés et les droits fondamentaux des personnes physiques, notamment leur vie privée, en ce qui concerne le traitement des données à caractère personnel, soient respectés par les institutions et organes communautaires. Il fixe aussi dans leurs grandes lignes certains aspects de cette mission. Ces responsabilités générales sont développées et précisées aux articles 46 et 47, lesquels comportent une énumération détaillée des fonctions et des compétences.

Cette présentation des attributions, fonctions et compétences suit, pour l'essentiel, le même schéma que pour les autorités nationales de contrôle: entendre et examiner les plaintes, effectuer des enquêtes, informer le responsable du traitement et les personnes concernées, effectuer des contrôles préalables lorsque les opérations de traitement présentent des risques particuliers, etc. Le règlement habilite le CEPD à obtenir accès à toutes les informations utiles et aux locaux pertinents lorsque cela est nécessaire pour ses enquêtes. Le CEPD peut aussi imposer des sanctions et saisir la Cour de justice. Ces activités de **supervision** sont examinées de façon plus approfondie dans le chapitre 2 du présent rapport.

Certaines tâches revêtent une nature particulière. La tâche consistant à conseiller la Commission et les autres institutions communautaires à propos des nouvelles dispositions législatives (confirmée à l'article 28, paragraphe 2, par l'obligation formelle qui est faite à la Commission de consulter le CEPD lorsqu'elle adopte une proposition de législation relative à la protection des données à caractère personnel) concerne aussi les projets de directive et les autres mesures applicables ou transposables au niveau national. Il s'agit d'une fonction stratégique qui permet au CEPD de se pencher, très tôt, sur les implications possibles au regard de la protection de la vie privée et d'envisager d'autres solutions éventuelles, y compris dans le troisième pilier (coopération policière et judiciaire en matière pénale). Surveiller les faits nouveaux qui présentent un intérêt et qui pourraient avoir une incidence sur la protection des données à caractère personnel constitue une autre tâche très importante. Ces activités **consultatives** du CEPD sont examinées plus en détail dans le chapitre 3 du présent rapport.

La coopération avec les autorités nationales de contrôle et la coopération avec les organes de contrôle relevant du troisième pilier sont de même nature. En tant que membre du groupe de l'article 29 qui a été institué pour conseiller la Commission et pour développer des politiques harmonisées, le CEPD apporte une contribution précieuse. La coopération avec les organes de contrôle relevant du troisième pilier lui permet d'observer les faits nouveaux qui surviennent dans ce contexte et de contribuer à l'élaboration d'un cadre plus cohérent et homogène pour la protection des données à caractère personnel, quel que soit le pilier ou le contexte particulier concerné. Cette **coopération** est traitée plus en détail dans le chapitre 4 du présent rapport.

## Annexe B

## Extrait du règlement (CE) n° 45/2001

**Article 41 — Le Contrôleur européen de la protection des données**

1. Il est institué une autorité de contrôle indépendante dénommée le Contrôleur européen de la protection des données.
2. En ce qui concerne le traitement de données à caractère personnel, le Contrôleur européen de la protection des données est chargé de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires.

Le Contrôleur européen de la protection des données est chargé de surveiller et d'assurer l'application des dispositions du présent règlement et de tout autre acte communautaire concernant la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par une institution ou un organe communautaire ainsi que de conseiller les institutions et organes communautaires et les personnes concernées sur toutes les questions concernant le traitement des données à caractère personnel. À ces fins, il exerce les fonctions prévues à l'article 46 et les compétences qui lui sont conférées à l'article 47.

**Article 46 — Fonctions**

Le Contrôleur européen de la protection des données:

- a) entend et examine les réclamations et informe la personne concernée des résultats de son examen dans un délai raisonnable;
- b) effectue des enquêtes, soit de sa propre initiative, soit sur la base d'une réclamation et informe les personnes concernées du résultat de ses enquêtes dans un délai raisonnable;
- c) contrôle et assure l'application du présent règlement et de tout autre acte communautaire relatifs à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par une institution ou un organe communautaire, à l'exclusion de la Cour de justice des Communautés européennes dans l'exercice de ses fonctions juridictionnelles;
- d) conseille l'ensemble des institutions et organes communautaires, soit de sa propre initiative, soit en réponse à une consultation, sur toutes les questions concernant le traitement de données à caractère personnel, en particulier avant l'élaboration par ces institutions et organes de règles internes relatives à la protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel;
- e) surveille les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications;
- f)
  - i) coopère avec les autorités nationales de contrôle mentionnées à l'article 28 de la directive 95/46/CE des pays auxquels cette directive s'applique dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes informations utiles, en demandant à une telle autorité ou à un tel organe d'exercer ses pouvoirs ou en répondant à une demande d'une telle autorité ou d'un tel organe;
  - ii) coopère également avec les organes de contrôle de la protection des données institués en vertu du titre VI du traité sur l'Union européenne en vue notamment d'améliorer la cohérence dans l'application des règles et procédures dont ils sont respectivement chargés d'assurer le respect;
- g) participe aux activités du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE;
- h) détermine, motive et rend publiques les exceptions, garanties, autorisations et conditions mentionnées à l'article 10, paragraphe 2, point b), paragraphes 4, 5 et 6, à l'article 12, paragraphe 2, à l'article 19 et à l'article 37, paragraphe 2;
- i) tient un registre des traitements qui lui ont été notifiés en vertu de l'article 27, paragraphe 2, et enregistrés conformément à l'article 27, paragraphe 5, et fournit les moyens d'accéder aux registres tenus par les délégués à la protection des données en application de l'article 26;

- j) effectue un contrôle préalable des traitements qui lui ont été notifiés;
- k) établit son règlement intérieur.

### Article 47 — Compétences

1. Le Contrôleur européen de la protection des données peut:
  - a) conseiller les personnes concernées dans l'exercice de leurs droits;
  - b) saisir le responsable du traitement en cas de violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, formuler des propositions tendant à remédier à cette violation et à améliorer la protection des personnes concernées;
  - c) ordonner que les demandes d'exercice de certains droits à l'égard des données soient satisfaites lorsque de telles demandes ont été rejetées en violation des articles 13 à 19;
  - d) adresser un avertissement ou une admonestation au responsable du traitement;
  - e) ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données lorsqu'elles

ont été traitées en violation des dispositions régissant le traitement de données à caractère personnel et la notification de ces mesures aux tiers auxquels les données ont été divulguées;

- f) interdire temporairement ou définitivement un traitement;
  - g) saisir l'institution ou l'organe concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;
  - h) saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité;
  - i) intervenir dans les affaires portées devant la Cour de justice des Communautés européennes.
2. Le Contrôleur européen de la protection des données est habilité à:
    - a) obtenir d'un responsable du traitement ou d'une institution ou d'un organe communautaire l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à ses enquêtes;
    - b) obtenir l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution ou un organe communautaire exerce ses activités s'il existe un motif raisonnable de supposer que s'y exerce une activité visée par le présent règlement.

## Annexe C

## LISTE DES ABRÉVIATIONS ET ACRONYMES

ACCP	Agence communautaire de contrôle des pêches
BCE	Banque centrale européenne
BEI	Banque européenne d'investissement
CC	Cour des comptes
CCR	Centre commun de recherche
CdR	Comité des régions
CdT	Centre de traduction des organes de l'Union européenne
CE	Communauté européenne
CEDH	convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales
CESE	Comité économique et social européen
CIG	Conférence intergouvernementale
CPD	coordinateur de la protection des données (Commission européenne uniquement)
DPA	autorité chargée de la protection des données
DPD	délégué à la protection des données
EEA	École européenne d'administration
EFSA	Autorité européenne de sécurité des aliments
EMEA	Agence européenne des médicaments
EMSA	Agence européenne pour la sécurité maritime
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
EPSO	Office européen de sélection du personnel
ETF	Fondation européenne pour la formation
Eurofound	Fondation européenne pour l'amélioration des conditions de vie et de travail
FIDE	fichier d'identification des dossiers d'enquêtes douanières
IMI	système d'information du marché intérieur
LCC	liste de conservation commune
LIBE	commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen
OCDE	Organisation de coopération et de développement économiques
OCVV	Office communautaire des variétés végétales
OEDT	Observatoire européen des drogues et des toxicomanies
OHMI	Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles)
OLAF	Office européen de lutte antifraude
PMO	Office de gestion et de liquidation des droits individuels
PNR	dossiers passagers (Passenger Name Record)
R & D	recherche et développement
RFID	identification par radiofréquence
SAI	service d'audit interne
SAR	système d'alerte rapide
SCPC	système de coopération en matière de protection des consommateurs
SID	système d'information douanier

SIS	système d'information Schengen
SWIFT	société mondiale de télécommunications financières interbancaires
Troisième pilier	coopération policière et judiciaire en matière pénale
UE	Union européenne
VIS	système d'information sur les visas
WP 29	groupe de l'article 29

## Annexe D

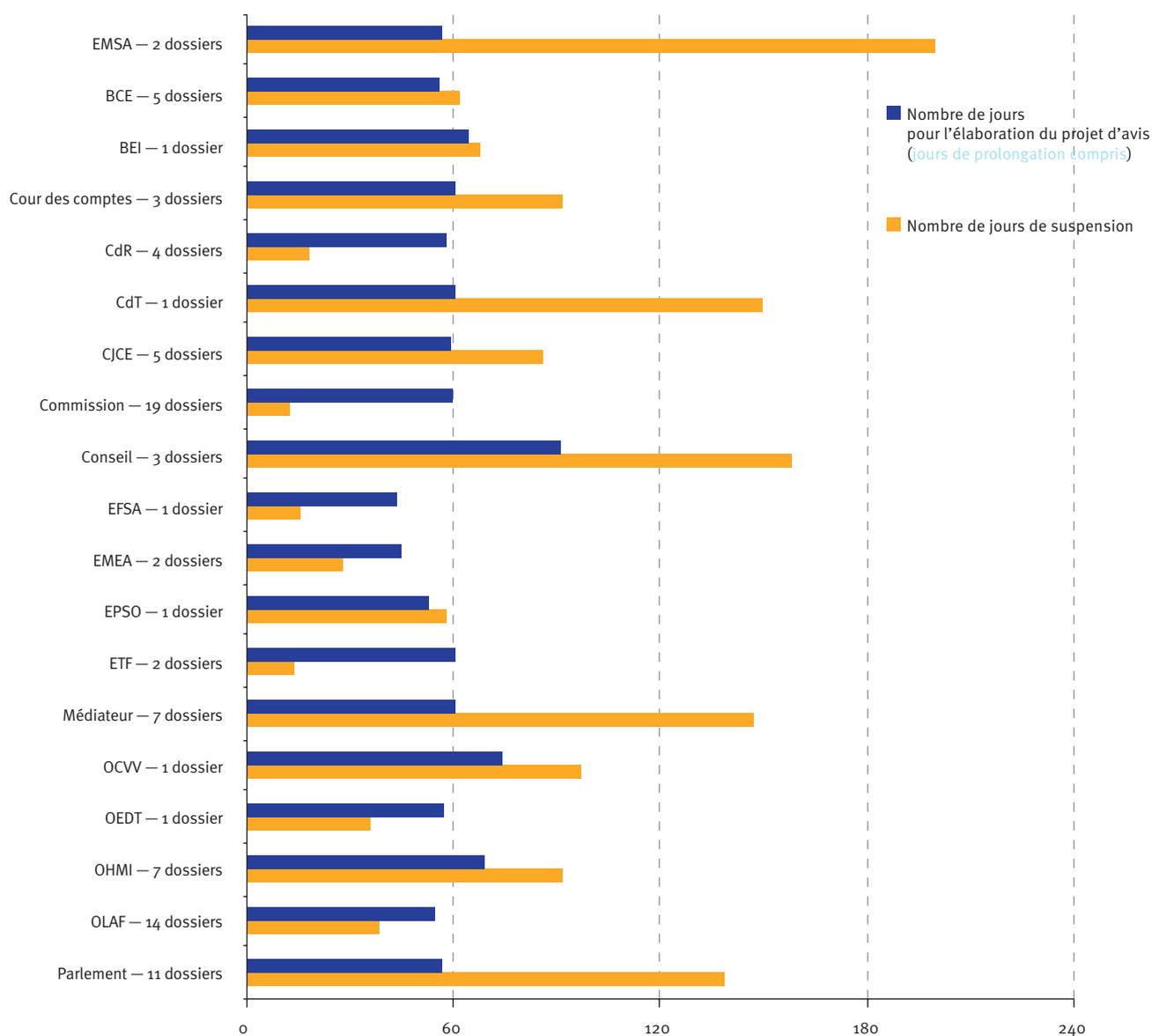
## Liste des délégués à la protection des données

Institutions et organes	Nom	Adresse électronique
Parlement européen	Jonathan STEELE	dg5data-protection@europarl.europa.eu
Conseil de l'Union européenne	Pierre VERNHES	data.protection@consilium.europa.eu
Commission européenne	Philippe RENAUDIÈRE	data-protection-officer@ec.europa.eu
Cour de justice	Marc SCHAUSS	dataprotectionofficer@curia.europa.eu
Cour des comptes	Jan KILB	data-protection@eca.europa.eu
Comité économique et social européen	Sofia FAKIRI	data.protection@eesc.europa.eu
Comité des régions	Petra CANDELLIER	data.protection@cor.europa.eu
Banque européenne d'investissement	Jean-Philippe MINNAERT	dataprotectionofficer@eib.org
Fonds européen d'investissement	Jobst NEUSS	j.neuss@eif.org
Banque centrale européenne	Martin BENISCH	DPO@ecb.int
Médiateur européen	Loïc JULIEN	dpo-euro-ombudsman@ombudsman.europa.eu
Contrôleur européen de la protection des données	Giuseppina LAURITANO	giuseppina.lauritano@edps.europa.eu
Office européen de lutte antifraude (OLAF)	Laraine LAUDATI	laraine.laudati@ec.europa.eu
Agence communautaire de contrôle des pêches (ACCP)	Rieke ARNDT	rieke.arndt@ext.ec.europa.eu
Office communautaire des variétés végétales (OCVV)	Véronique DOREAU	doreau@cpvo.europa.eu
Agence exécutive «Éducation, audiovisuel et culture»	Hubert MONET	hubert.monet@ec.europa.eu
Agence européenne pour la reconstruction (AER)	Martin DISCHENDORFER	martin.dischendorfer@ear.europa.eu
Agence européenne pour la sécurité et la santé au travail (EU-OSHA)	Terry TAYLOR	taylor@osha.europa.eu
Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures (Frontex)	Sakari VUORENSOLA	sakari.vuorensola@frontex.europa.eu
Agence européenne de la sécurité aérienne (AESA)	Arthur BECKAND	arthur.beckand@easa.europa.eu
Centre européen de prévention et de contrôle des maladies (ECDC)	Elisabeth ROBINO	elisabeth.robino@ecdc.europa.eu
Centre européen pour le développement de la formation professionnelle (Cedefop)	Spyros ANTONIOU	spyros.antoniou@cedefop.europa.eu
Agence européenne pour l'environnement (AEE)	Gordon McINNES	gordon.mcinnis@eea.europa.eu
Autorité européenne de sécurité des aliments (EFSA)	Claus REUNIS	dataprotectionofficer@efsa.europa.eu

Institutions et organes	Nom	Adresse électronique
Fondation européenne pour l'amélioration des conditions de vie et de travail (Eurofound)	Markus GRIMMEISEN	mgr@eurofound.europa.eu
Autorité de surveillance du GNSS européen (GSA)	Dimitri NICOLAÏDES	dimitri.nicolaides@gsa.europa.eu
Agence européenne pour la sécurité maritime (EMSA)	Malgorzata NESTEROWICZ	malgorzata.nesterowicz@emsa.europa.eu
Agence européenne des médicaments (EMA)	Vincenzo SALVATORE	data.protection@emea.europa.eu
Observatoire européen des drogues et des toxicomanies (OEDT)	Cécile MARTEL	cecile.martel@emcdda.europa.eu
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)	Andreas MITRAKAS	dataprotection@enisa.europa.eu
Agence ferroviaire européenne (AFE)	Zografia PYLORIDOU	zographia.pyloridou@era.europa.eu
Fondation européenne pour la formation (ETF)	à désigner	
Agence des droits fondamentaux de l'Union européenne (FRA)	Nikolaos FIKATAS	nikolaos.fikatas@fra.europa.eu
Agence exécutive pour la compétitivité et l'innovation	Olivier CORNU	olivier.cornu@ext.ec.europa.eu
Agence exécutive pour le programme de santé publique	Eva LÄTTI	eva.latti@ec.europa.eu
Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles) (OHMI)	Luc DEJAÏFFE	dataprotectionofficer@oami.europa.eu
Centre de traduction des organes de l'Union européenne (CdT)	Benoît VITALE	data-protection@cdt.europa.eu

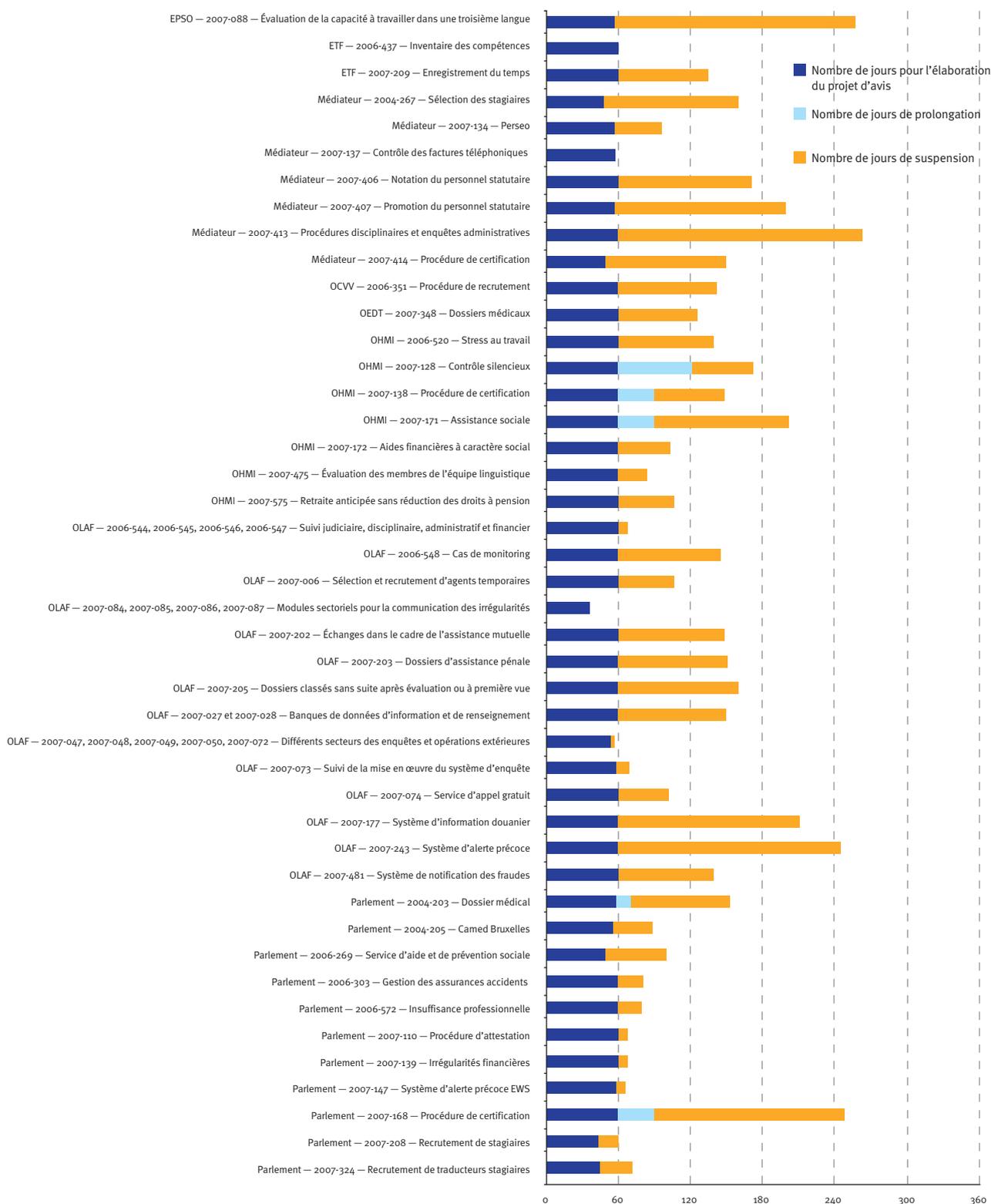
Annexe E

## Délais de traitement des contrôles préalables par dossier et par institution

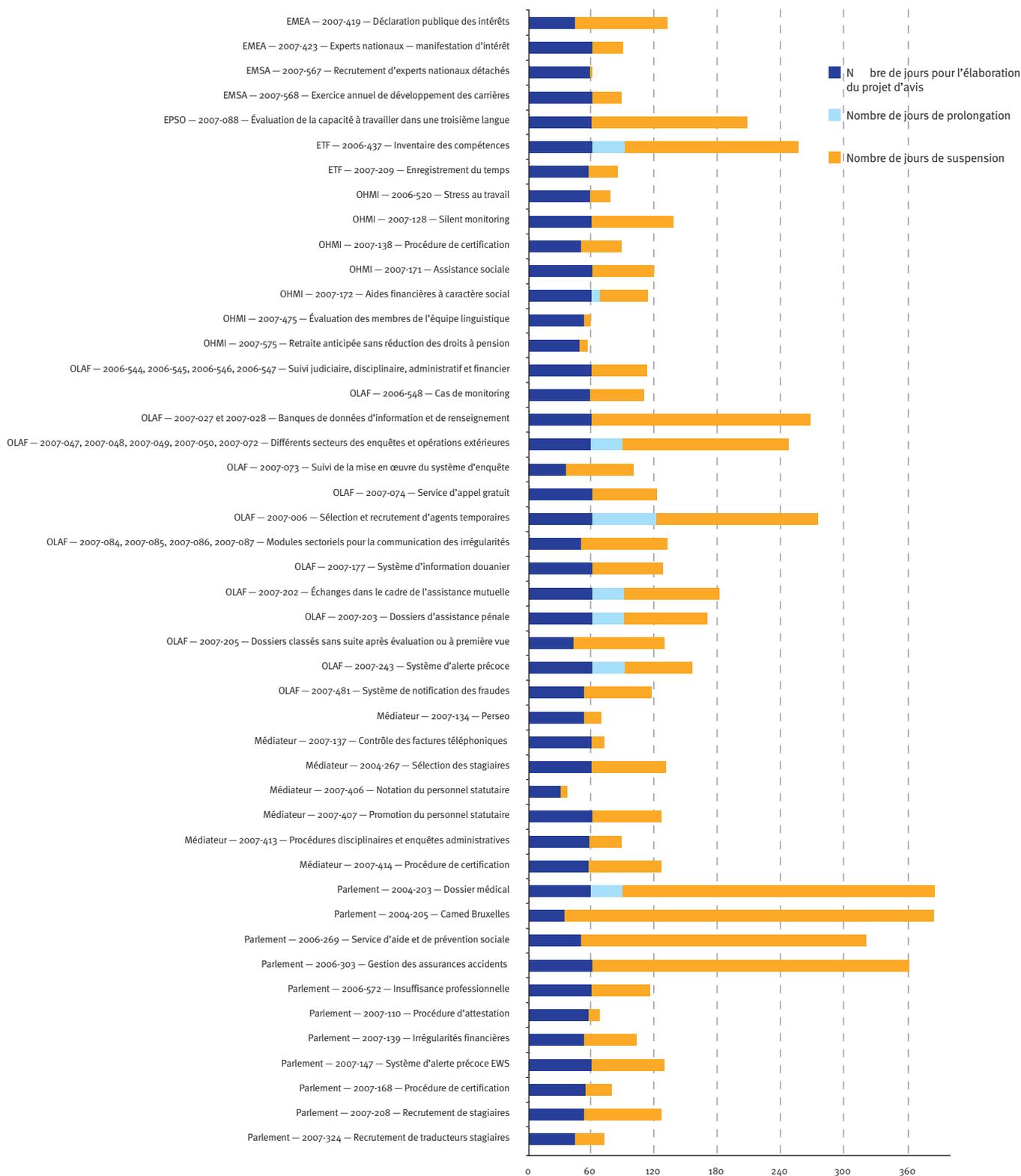


NB: Le mois d'août n'est pas inclus dans les jours pris pour l'élaboration des projets d'avis concernant les dossiers a posteriori reçus avant le 1<sup>er</sup> septembre 2007.

**Avis publiés en 2007 (I)**



**Avis publiés en 2007 (II)**



NB: Le mois d'août n'est pas inclus dans les jours pris pour l'élaboration des projets d'avis concernant les dossiers a posteriori reçus avant le 1<sup>er</sup> septembre 2007.

## Annexe F

# Liste des avis rendus à la suite d'un contrôle préalable

### **New flexitime AGRI — Commission**

Réponse du 19 décembre 2007 à une notification de contrôle préalable relative au «New flexitime AGRI» (dossier 2007-680)

### **Service de notification des fraudes — OLAF**

Avis du 18 décembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Service de notification des fraudes» (dossier 2007-481)

### **Développement de carrière — Agence européenne pour la sécurité maritime**

Avis du 17 décembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Développement de carrière annuel» (dossier 2007-568)

### **Conseiller social — Banque centrale européenne**

Avis du 6 décembre 2007 sur la notification d'un contrôle préalable à propos des données traitées par le conseiller social (dossier 2007-489)

### **Dossiers sociaux — CESE et CdR**

Avis du 6 décembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Dossiers sociaux» (dossier 2007-355)

### **Procédure de notation — Comité des régions**

Avis du 4 décembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure de notation des fonctionnaires et agents» (dossier 2007-356)

### **Procédure d'attestation — Comité des régions**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure d'attestation» (dossier 2007-352)

### **Procédure d'invalidité — Commission**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure d'invalidité — services médicaux Bruxelles-Luxembourg» (dossier 2007-125)

### **Grève et actions assimilables — Conseil**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Gestion administrative en cas de grève et actions assimilables: retenues sur traitement et mesures de réquisitions» (dossier 2004-249)

### **Données de dosimétrie au CCR-IRMM — Commission**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Données de dosimétrie au CCR-IRMM à Geel» (dossier 2007-325)

### **Certification — Comité des régions**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure de certification» (dossier 2007-353)

### **Examen ophtalmologique — Cour des comptes**

Avis du 29 novembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Examen ophtalmologique de suivi des personnes travaillant sur écran» (dossier 2007-303)

**Retraite anticipée — OHMI**

Avis du 22 novembre 2007 sur la notification d'un contrôle préalable concernant la procédure de retraite anticipée sans réduction des droits à pension (dossier 2007-575)

**Bases de données de renseignement — OLAF**

Avis du 21 novembre 2007 sur la notification d'un contrôle préalable concernant le pool de données en matière d'information et de renseignement («Information and Intelligence Data Pool») et les bases de données de renseignement («Intelligence Databases») (dossiers joints 2007-27 et 2007-28)

**Recrutement des experts nationaux détachés — EMSA**

Avis du 20 novembre 2007 sur la notification d'un contrôle préalable concernant la procédure de recrutement des experts nationaux détachés (dossier 2007-567)

**Recrutement d'agents temporaires — OLAF**

Avis du 14 novembre 2007 sur la notification d'un contrôle préalable concernant la sélection et le recrutement par l'OLAF de ses agents temporaires (dossier 2007-6)

**Évaluation des membres de l'équipe linguistique — OHMI**

Avis du 12 novembre 2007 sur la notification d'un contrôle préalable concernant l'évaluation des membres de l'équipe linguistique (dossier 2007-475)

**Traitement de données à caractère personnel par les services sociaux — Cour des comptes**

Avis du 8 novembre 2007 sur la notification d'un contrôle préalable à propos du traitement des données à caractère personnel par les services sociaux (dossier 2007-302)

**Experts nationaux — EMEA**

Avis du 26 octobre 2007 sur la notification d'un contrôle préalable concernant les manifestations d'intérêt des experts nationaux (dossier 2007-423)

**Certification — Médiateur**

Avis du 24 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure de certification» (dossier 2007-414)

**Promotions — Médiateur**

Avis du 22 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Promotion du personnel statutaire» (dossier 2007-407)

**Le flexitime à la DG Société de l'information et médias — Commission**

Avis du 19 octobre 2007 sur la notification d'un contrôle préalable à propos de la mise en œuvre d'un flexitime spécifique à la DG Société de l'information et médias (dossier 2007-218)

**Échanges d'informations relevant de l'assistance mutuelle — OLAF**

Avis du 19 octobre 2007 sur la notification d'un contrôle préalable à propos des échanges d'informations relevant de l'assistance mutuelle (dossier 2007-202)

**Procédure disciplinaire et enquête administrative — Médiateur**

Avis du 17 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure disciplinaire et enquêtes administratives» (dossier 2007-413)

**Irrégularités financières — Cour de justice**

Avis du 17 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Instance spécialisée en matière d'irrégularités financières» (dossier 2007-433)

#### **Dossiers d'assistance pénale — OLAF**

Avis du 12 octobre 2007 sur la notification d'un contrôle préalable à propos des dossiers d'assistance pénale (dossier 2007-203)

#### **Absences pour maladie — Commission**

Avis du 11 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Contrôle des absences pour maladie Bruxelles-Luxembourg» (dossier 2004-226)

#### **Sysper 2: promotions — Commission**

Avis du 9 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Sysper 2: promotions» (dossier 2007-192)

#### **Système d'alerte précoce — OLAF**

Avis du 4 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Système d'alerte précoce» (dossier 2007-243)

#### **Indemnités spéciales au Centre commun de recherche — Commission**

Avis du 4 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Vérification des déclarations concernant les indemnités spéciales au Centre commun de recherche» (dossier 2007-328)

#### **Harcèlement — Cour de justice**

Avis du 4 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure de harcèlement» (dossier 2007-440)

#### **Enquêtes externes — OLAF**

Avis du 4 octobre 2007 sur cinq notifications de contrôle préalable à propos des enquêtes externes (dossiers 2007-47, 2007-48, 2007-49, 2007-50, 2007-72)

#### **Procédure de certification — Cour de justice**

Avis du 3 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure de certification» (dossier 2007-434)

#### **Dossiers classés sans suite — OLAF**

Avis du 3 octobre 2007 sur la notification d'un contrôle préalable à propos des dossiers classés sans suite après évaluation préalable et des dossiers classés sans suite à première vue (dossier 2007-205)

#### **Procédure d'attestation — Cour de justice**

Avis du 3 octobre 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure d'attestation» (dossier 2007-435)

#### **Sélection de hauts fonctionnaires — Commission**

Avis du 17 septembre 2007 sur la notification d'un contrôle préalable à propos de la sélection de hauts fonctionnaires à la Commission (dossier 2007-193)

#### **Visites médicales — OEDT**

Avis du 13 septembre 2007 sur la notification d'un contrôle préalable à propos des visites médicales d'engagement et des visites médicales annuelles (dossier 2007-348)

#### **Conflits d'intérêts des conseillers spéciaux — Commission**

Avis du 11 septembre 2007 sur la notification d'un contrôle préalable concernant la vérification de l'absence de conflits d'intérêts des conseillers spéciaux et la publication sur le site web Europa (dossier 2007-294)

**Service médical — Commission**

Avis du 10 septembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Gestion des activités du service médical — Bruxelles-Luxembourg — notamment via l'application informatique Sermed» (dossier 2004-232)

**Habilitation de sécurité — Banque centrale européenne**

Avis du 7 septembre 2007 sur la notification d'un contrôle préalable concernant l'application des règles d'habilitation (dossier 2007-371)

**Exercices de redéploiement — Commission**

Avis du 5 septembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Interventions dans le cadre des exercices de redéploiement» (dossier 2007-278)

**Évaluation de la troisième langue — EPSO**

Avis du 4 septembre 2007 sur la notification d'un contrôle préalable à propos du dossier «Évaluation de la capacité à travailler dans une troisième langue (application de l'article 45, paragraphe 2, du statut)» (dossier 2007-88)

**Dossiers médicaux et gestion du temps — Banque européenne d'investissement**

Avis du 3 août 2007 sur la notification d'un contrôle préalable concernant la modification du traitement de données relatives à la «gestion du temps» et aux «dossiers médicaux» (dossier 2007-373)

**Évaluation du personnel — Médiateur**

Avis du 3 août 2007 sur la notification d'un contrôle préalable concernant l'évaluation du personnel (dossier 2007-406)

**Recrutement de traducteurs stagiaires — Parlement**

Avis du 31 juillet 2007 sur la notification d'un contrôle préalable concernant le recrutement de traducteurs stagiaires (dossier 2007-324)

**Recrutement de stagiaires — Parlement**

Avis du 31 juillet 2007 sur la notification d'un contrôle préalable concernant le recrutement de stagiaires (dossier 2007-208)

**Base de données «Amiante» — Commission**

Avis du 27 juillet 2007 sur la notification d'un contrôle préalable à propos du dossier «Dépistage et suivi des cas d'asbestose — Base des données «Amiante» (service médical et interventions psychosociales BXL)» (dossier 2004-227)

**Crèches — Commission**

Avis du 27 juillet 2007 sur la notification d'un contrôle préalable à propos du dossier «Gestion des crèches et garderies à Bruxelles» (dossier 2007-148)

**Couverture des risques d'accident et de maladie professionnelle — Commission**

Avis du 27 juillet 2007 sur la notification d'un contrôle préalable concernant l'administration de l'assurance accident et maladie professionnelle (dossier 2007-157)

**Aides sociales (ISPRA) — Commission**

Avis du 24 juillet 2007 sur la notification d'un contrôle préalable à propos des aides sociales, financières et aide pratique (dossier 2007-304)

**Système d'information douanier — OLAF**

Avis du 24 juillet 2007 sur la notification d'un contrôle préalable concernant le système d'information douanier (SID) (dossier 2007-177)

**Assistance sociale — OHMI**

Avis du 23 juillet 2007 sur la notification d'un contrôle préalable concernant l'octroi de l'assistance sociale (dossier 2007-171)

**Observateurs électoraux («le Roster») — Commission**

Avis du 23 juillet 2007 sur la notification d'un contrôle préalable concernant la liste d'enregistrement des observateurs électoraux («le Roster») qui figure sur le site web EUROPA (dossier 2007-244)

**Procédures de passation des marchés publics — Conseil**

Avis du 19 juillet 2007 sur la notification d'un contrôle préalable concernant les procédures de passation des marchés publics (dossier 2007-275)

**Fonction d'enquête — OLAF**

Avis du 19 juillet 2007 sur la notification d'un contrôle préalable concernant le contrôle régulier sur l'exécution de la fonction d'enquête (dossier 2007-73)

**Contrôle silencieux — OHMI**

Avis du 18 juillet 2007 sur la notification d'un contrôle préalable concernant la procédure de contrôle silencieux (dossier 2007-128)

**Système d'alerte précoce EWS — Parlement**

Avis du 16 juillet 2007 sur la notification d'un contrôle préalable à propos du dossier «Système d'alerte précoce/early warning system (EWS)» (dossier 2007-147)

**Cas de monitoring — OLAF**

Avis du 11 juillet 2007 sur la notification d'un contrôle préalable concernant les cas de monitoring (dossier 2006-548)

**Régime d'assurance maladie — Commission**

Avis du 10 juillet 2007 sur la notification d'un contrôle préalable concernant la gestion du régime d'assurance maladie commun aux institutions des Communautés européennes — RCAM (dossier 2004-238)

**Aides pécuniaires à caractère social — OHMI**

Avis du 3 juillet 2007 sur la notification d'un contrôle préalable concernant l'octroi d'«aides pécuniaires à caractère social» (dossier 2007-172)

**Système d'information antifraude AFIS — OLAF**

Avis du 29 juin 2007 sur la notification d'un contrôle préalable concernant l'utilisation de modules sectoriels spécialisés dans le cadre du Système d'information antifraude (AFIS) (dossiers 2007-84, 2007-85, 2007-86 et 2007-87)

**Système d'enregistrement du temps de travail — ETF**

Avis du 21 juin 2007 sur la notification d'un contrôle préalable concernant le système d'enregistrement du temps de travail au sein de la Fondation (dossier 2007-209)

**Dossier médical (Bruxelles) — Parlement**

Avis du 14 juin 2007 sur la notification d'un contrôle préalable à propos du dossier «Camed-Bruxelles» (dossier 2004-205)

**Dossier médical (Luxembourg) — Parlement**

Avis du 14 juin 2007 sur la notification d'un contrôle préalable à propos du dossier «Dossiers médicaux — Luxembourg» (dossier 2004-203)

**Inventaire des compétences — Fondation européenne pour la formation**

Avis du 13 juin 2007 sur la notification d'un contrôle préalable concernant l'inventaire des compétences de l'ETF (dossier 2006-437)

**Procédure de sélection des stagiaires — Conseil**

Avis du 12 juin 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure de sélection des stagiaires au secrétariat général du Conseil de l'Union européenne» (dossier 2007-217)

**Irrégularités financières — Parlement**

Avis du 12 juin 2007 sur la notification d'un contrôle préalable à propos du dossier «Panel d'irrégularités financières» (dossier 2007-139)

**Service d'appel gratuit — OLAF**

Avis du 6 juin 2007 sur la notification d'un contrôle préalable concernant un service d'appel gratuit (dossier 2007-74)

**Procédure de certification — Parlement**

Avis du 6 juin 2007 sur la notification d'un contrôle préalable concernant la procédure de certification (dossier 2007-168)

**Procédure de certification — OHMI**

Avis du 6 juin 2007 sur la notification d'un contrôle préalable à propos du dossier «Procédure de certification» (dossier 2007-138)

**Procédure de recrutement — Banque centrale européenne**

Avis du 4 juin 2007 sur la notification d'un contrôle préalable concernant la procédure de recrutement (dossier 2007-3)

**Vérification des factures téléphoniques — Médiateur**

Avis du 14 mai 2007 sur la notification d'un contrôle préalable concernant la vérification des factures téléphoniques (dossier 2007-137)

**Perseo — Médiateur**

Avis du 7 mai 2007 sur la notification d'un contrôle préalable concernant Perseo (Dossier 2007-134)

**Stress au travail — OHMI**

Avis du 2 mai 2007 concernant une étude sur le stress au travail (dossier 2006-520)

**Assistance sociale — Parlement**

Avis du 30 avril 2007 sur la notification d'un contrôle préalable à propos du dossier «Assistance sociale et conseil en cas de dépendances» (dossier 2006-269)

**Assurances accidents — Parlement**

Avis du 30 avril 2007 sur la notification d'un contrôle préalable à propos du dossier «Gestion des assurances accidents» (dossier 2006-303)

**Procédure d'attestation — Parlement**

Avis du 26 avril 2007 sur la notification d'un contrôle préalable concernant la procédure d'attestation (dossier 2007-110)

**Procédure d'amélioration en cas d'insuffisance professionnelle — Parlement**

Avis du 10 avril 2007 sur la notification d'un contrôle préalable concernant la procédure d'amélioration en cas d'insuffisance professionnelle (dossier 2006-572)

**Gestion du temps — Commission**

Avis du 29 mars 2007 sur la notification d'un contrôle préalable à propos du dossier «Sysper 2: module Time management» (dossier 2007-63)

**Opérations de traitement de données de suivi — OLAF**

Avis du 26 mars 2007 sur les opérations de traitement de données dans le cadre d'un suivi disciplinaire, administratif, judiciaire ou financier (dossiers 2006-544, 2006-545, 2006-546, 2006-547)

**Visites médicales — Autorité européenne de sécurité des aliments**

Avis du 23 mars 2007 sur la notification d'un contrôle préalable à propos des visites médicales d'engagement et des visites médicales annuelles de l'EFSA (dossier 2006-365)

**Retraite anticipée — Commission**

Avis du 20 mars 2007 sur la notification d'un contrôle préalable à propos du dossier «Exercice annuel de retraite anticipée sans réduction des droits à pension» (dossier 2006-577)

**Utilisation des téléphones portables — Banque centrale européenne**

Avis du 26 février 2007 sur la notification d'un contrôle préalable concernant les procédures d'enquête relatives à l'utilisation des téléphones portables (dossier 2004-272)

**Aides sociales — Cour de justice**

Avis du 21 février 2007 sur la notification d'un contrôle préalable à propos des aides sociales (dossier 2006-561)

**Utilisation des téléphones de service — Banque centrale européenne**

Avis du 13 février 2007 sur la notification d'un contrôle préalable concernant les procédures d'enquête relatives à l'utilisation de téléphones de service (dossier 2004-271)

**Procédure de recrutement — Office communautaire des variétés végétales**

Avis du 2 février 2007 sur la notification d'un contrôle préalable concernant la procédure de recrutement (dossier 2006-351)

**Insuffisance professionnelle — Cour des comptes**

Avis du 18 janvier 2007 sur la notification d'un contrôle préalable à propos du dossier «Maintenance du niveau des prestations en cas d'insuffisance professionnelle» (dossier 2006-534)

## Annexe G

## Liste des avis sur des propositions législatives

### Dossiers passagers européens

Avis du 20 décembre 2007 sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives

### Identification par radiofréquences (RFID)

Avis du 20 décembre 2007 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «L'identification par radiofréquence (RFID) en Europe: vers un cadre politique» [COM(2007) 96]

### Mise en œuvre de l'initiative de Prüm

Avis du 19 décembre 2007 sur l'initiative de la République fédérale d'Allemagne, en vue de l'adoption d'une décision du Conseil concernant la mise en œuvre de la décision 2007/.../JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière

### Transporteurs par route

Avis du 12 septembre 2007 sur la proposition de règlement établissant des règles communes sur les conditions à respecter pour exercer la profession de transporteur par route, JO C 14 du 19.1.2008, p. 1

### Statistiques communautaires sur la santé

Avis du 5 septembre 2007 sur la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail [COM(2007) 46 final], JO C 295 du 7.12.2007, p. 1

### Mise en application de la directive sur la protection des données

Avis du 25 juillet 2007 sur la communication de la Commission au Parlement européen et au Conseil relative au suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données, JO C 255 du 27.10.2007, p. 1

### Protection des données dans le cadre du troisième pilier

Troisième avis du 27 avril 2007 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO C 139 du 23.6.2007, p. 1

### Financement de la politique agricole commune

Avis du 10 avril 2007 sur la proposition de règlement du Conseil portant sur la modification du règlement (CE) n° 1290/2005 relatif au financement de la politique agricole commune [COM(2007) 122 final], JO C 134 du 16.6.2007, p. 1

### Coopération transfrontière (traité de Prüm)

Avis du 4 avril 2007 sur l'initiative de 15 États membres en vue de l'adoption de la décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, JO C 169 du 21.7.2007, p. 2

### Coordination des systèmes de sécurité sociale

Avis du 6 mars 2007 concernant la proposition de règlement fixant les modalités d'application du règlement (CE) n° 883/2004 portant sur la coordination des systèmes de sécurité sociale [COM(2006) 16 final], JO C 91 du 26.4.2007, p. 15

**Bonne application des réglementations douanière et agricole**

Avis du 22 février 2007 sur la proposition de règlement modifiant le règlement (CE) n° 515/97 du Conseil relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole [COM(2006) 866 final], JO C 94 du 28.4.2007, p. 3

**Office européen de police**

Avis du 16 février 2007 sur la proposition de décision du Conseil portant création de l'Office européen de police (Europol) [COM(2006) 817 final], JO C 255 du 27.10.2007, p. 13

## Annexe H

## Composition du secrétariat du CEPD

**Domaines placés sous la responsabilité directe du CEPD et du Contrôleur adjoint**• **Supervision**

Sophie LOUVEAUX Administratrice/Conseillère juridique	Delphine HAROU (*) Assistante Supervision
Rosa BARCELÓ Administratrice/Conseillère juridique	Xanthi KAPSOSIDERI Assistante Supervision
Zsuzsanna BELENYESSY Administratrice/Conseillère juridique	Sylvie LONGRÉE Assistante Supervision
Eva DIMOVNÉ KERESZTES Administratrice/Conseillère juridique	Kim Thien LÊ Assistante Secrétariat
Maria Verónica PEREZ ASINARI Administratrice/Conseillère juridique	Thomas GREMEL Assistant Supervision
Jaroslav LOTARSKI Administrateur/Conseiller juridique	Stephen McCARTNEY Expert national/Conseiller juridique (de février 2007 à novembre 2007)
Tereza STRUNCOVA Administratrice/Conseillère juridique	Endre SZABÓ Expert national/Conseiller juridique (jusqu'en juillet 2007)
György HALMOS (*) Expert national/Conseiller juridique (depuis septembre 2007)	

• **Politique et information**

Hielke HIJMANS Administrateur/Conseiller juridique	Nathalie VANDELLE (*) Administratrice/Attachée de presse
Laurent BESLAY Administrateur/Conseiller Technologies	Per SJÖNELL (*) Administrateur/Attaché de presse (jusqu'en août 2007)
Bénédicte HAVELANGE Administratrice/Conseillère juridique	Martine BLONDEAU (*) Assistante Documentation
Alfonso SCIROCCO Administrateur/Conseiller juridique	Andrea BEACH Assistante Secrétariat
Michael VANFLETEREN Administrateur/Conseiller juridique	Matteo BONFANTI Stagiaire (d'octobre 2007 à janvier 2008)
Anne-Christine LACOSTE Administratrice/Conseillère juridique	Marie MCGINLEY Stagiaire (de mars à juillet 2007)

(\*) Unité «Information».



Le Contrôleur européen de la protection des données et le Contrôleur adjoint, entourés de leurs collaborateurs.

**Unité «Personnel/Budget/Administration»**

Monique LEENS-FERRANDO  
Chef d'unité

• **Ressources humaines/Administration**

Giuseppina LAURITANO  
Administratrice/Conseillère Questions  
statutaires et Audits/Déleguée à la protection  
des données

Vittorio MASTROJENI  
Assistant Ressources humaines

Anne LEVÉCQUE  
Assistante Ressources humaines

Anne-Françoise REYNDERS  
Assistante Ressources humaines

• **Budget et finances**

Tonny MATHIEU  
Administrateur financier

Raja ROY  
Assistante Questions financières et  
Comptabilité

Valérie LEAU  
Assistante Comptabilité

## Annexe I

## Liste des accords et décisions administratifs

**Accord administratif** signé par les secrétaires généraux du Parlement européen, du Conseil et de la Commission et le Contrôleur européen de la protection des données (24 juin 2004). Prorogation de cet accord signée le 11 décembre 2006.

### Liste des accords au niveau des services signés par le CEPD avec d'autres institutions

- Accord au niveau des services avec la Commission (bureau des stages de la DG Éducation et culture; DG Personnel et administration; DG Emploi, affaires sociales et égalité des chances)
- Accord au niveau des services avec le Conseil
- Accord au niveau des services avec l'École européenne d'administration (EAS)
- Accord administratif entre le CEPD et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)
- Accord relatif à l'harmonisation du coût des cours de langue interinstitutionnels
- Accords bilatéraux entre le Parlement européen et le CEPD mettant en œuvre l'accord administratif du 24 juin 2004, prorogé le 11 décembre 2006

### Liste des décisions adoptées par le CEPD

Décision du 12 janvier 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière d'allocations familiales

Décision du 27 mai 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution relatives au programme de stages

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de travail à temps partiel

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de congés

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution concernant les critères applicables au classement en échelon lors de la nomination ou de la prise de fonctions

Décision du 15 juin 2005 du Contrôleur européen de la protection des données portant adoption de l'horaire flexible avec possibilité de récupération des heures supplémentaires prestées

Décision du 22 juin 2005 du Contrôleur européen de la protection des données portant adoption d'une réglementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes

Décision du 1<sup>er</sup> juillet 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de congé familial

Décision du 15 juillet 2005 du Contrôleur européen de la protection des données portant adoption de la réglementation commune relative à la couverture des risques de maladie des fonctionnaires des Communautés européennes

Décision du 25 juillet 2005 du Contrôleur européen de la protection des données portant dispositions d'exécution en matière de congé de convenance personnelle des fonctionnaires et de congé sans rémunération des agents temporaires et agents contractuels des Communautés européennes

Décision du 25 juillet 2005 du Contrôleur européen de la protection des données relative aux activités extérieures et aux mandats

Décision du 26 octobre 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution relatives à l'allocation de foyer par décision spéciale

Décision du 26 octobre 2005 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de détermination du lieu d'origine

Décision du 7 novembre 2005 du Contrôleur européen de la protection des données établissant un système de contrôle interne au sein du CEPD

Décision du 10 novembre 2005 du Contrôleur européen de la protection des données relative au régime applicable aux experts nationaux détachés auprès de ses services

Décision du 16 janvier 2006 modifiant la décision du 22 juin 2005 du Contrôleur européen de la protection des données portant adoption d'une réglementation commune relative à la couverture des risques d'accident et de maladie professionnelle des fonctionnaires des Communautés européennes

Décision du 16 janvier 2006 modifiant la décision du 15 juillet 2005 du Contrôleur européen de la protection des données portant adoption d'une réglementation commune relative à la couverture des risques de maladie des fonctionnaires des Communautés européennes

Décision du 26 janvier 2006 du Contrôleur européen de la protection des données portant adoption de la réglementation fixant les modalités d'octroi d'une aide financière complétant la pension d'un conjoint survivant affecté d'une maladie grave ou prolongée ou souffrant d'un handicap

Décision du 8 février 2006 du Contrôleur européen de la protection des données relative à la mise en place d'un comité du personnel au CEPD

Décision du 9 septembre 2006 du Contrôleur européen de la protection des données adoptant la réglementation fixant les modalités d'application de l'article 45, paragraphe 2, du statut

Décision du 30 janvier 2007 du Contrôleur européen de la protection des données portant nomination du délégué à la protection des données du CEPD

Décision du 30 mars 2007 du Contrôleur européen de la protection des données portant adoption des dispositions générales d'exécution relatives à la notation du personnel

Décision du 18 juillet 2007 du Contrôleur européen de la protection des données portant adoption de la politique de formation interne

Décision du 12 septembre 2007 du Contrôleur européen de la protection des données relative aux conditions et modalités des enquêtes internes en matière de lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts des Communautés

Décision du 1<sup>er</sup> octobre 2007 du Contrôleur européen de la protection des données portant nomination du comptable du CEPD

Décision du 1<sup>er</sup> octobre 2007 du Contrôleur européen de la protection des données pour la mise en œuvre de l'article 4 de l'annexe VIII du statut relatif aux droits à pension

Décision du 1<sup>er</sup> octobre 2007 du Contrôleur européen de la protection des données pour la mise en œuvre des articles 11 et 12 de l'annexe VIII du statut relatif au transfert des droits à pension

Décision du 1<sup>er</sup> octobre 2007 du Contrôleur européen de la protection des données pour la mise en œuvre de l'article 22, paragraphe 4, de l'annexe XIII du statut relatif aux droits à pension

Décision du 9 novembre 2007 du Contrôleur européen de la protection des données portant nomination de l'auditeur interne du CEPD

Décision du 26 novembre 2007 du Contrôleur européen de la protection des données portant dispositions générales d'exécution en matière de promotions

Le Contrôleur européen de la protection des données

**Rapport annuel 2007**

Luxembourg: Office des publications officielles des Communautés européennes

2008 — 102 p. — 21 × 29,7 cm

ISBN 978-92-95030-42-8



### **Comment vous procurer les publications de l'Union européenne?**

Vous trouverez les publications de l'Office des publications disponibles à la vente sur le site de l'EU Bookshop (<http://bookshop.europa.eu/>), où vous pourrez passer commande auprès du bureau de vente de votre choix.

Vous pouvez également demander la liste des points de vente de notre réseau mondial par télécopie au (352) 29 29-42758.



LE CONTRÔLEUR EUROPÉEN  
DE LA PROTECTION DES DONNÉES

QT-AA-08-001-FR-C

*Le gardien européen  
de la protection des données personnelles*

**[www.edps.europa.eu](http://www.edps.europa.eu)**