

# Rapport annuel

## 2008



CONTRÔLEUR EUROPÉEN  
DE LA PROTECTION DES DONNÉES





# Rapport annuel

## 2008



CONTRÔLEUR EUROPÉEN  
DE LA PROTECTION DES DONNÉES

Europe Direct is a service to help you find answers  
to your questions about the European Union

Freephone number (\*):  
**00 800 6 7 8 9 10 11**

(\* Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (<http://europa.eu>).

Cataloguing data can be found at the end of this publication.

Luxembourg: Office for Official Publications of the European Communities, 2009

ISBN 978-92-79-11147-1

© Photos: Sylvie Picart-Longrée et iStockphoto

© European Communities, 2008

Reproduction is authorised provided the source is acknowledged.

*Printed in Italy*

PRINTED ON WHITE CHLORINE-FREE PAPER

# Sommaire

Guide de l'utilisateur	7
Mandat du CEPD	9
Avant-propos	11
1. Bilan et perspectives	13
<b>1.1. Aperçu général de 2008</b>	<b>13</b>
<b>1.2 Résultats obtenus en 2008</b>	<b>15</b>
<b>1.3 Objectifs en 2009</b>	<b>16</b>
2. Supervision	17
<b>2.1. Introduction</b>	<b>17</b>
<b>2.2. Délégués à la protection des données</b>	<b>17</b>
<b>2.3. Contrôles préalables</b>	<b>19</b>
2.3.1. Base juridique	19
2.3.2. Procédure	19
2.3.3. Évaluation quantitative	21
2.3.4. Principales questions soulevées par les dossiers examinés <i>a posteriori</i>	25
2.3.5. Principales questions soulevées par les cas de contrôle préalable	31
2.3.6. Consultations quant à la nécessité d'un contrôle préalable	34
2.3.7. Notifications non soumises au contrôle préalable ou retirées	35
2.3.8. Suivi des avis relatifs aux contrôles préalables	36
2.3.9. Conclusions et perspectives	37
<b>2.4. Plaintes</b>	<b>37</b>
2.4.1. Introduction	37
2.4.2. Plaintes déclarées recevables	38
2.4.3. Plaintes déclarées irrecevables : principaux motifs d'irrecevabilité	42
2.4.4. Collaboration avec le médiateur européen	43
2.4.5. Travaux complémentaires dans le domaine des plaintes	44
<b>2.5. Politique d'inspection</b>	<b>44</b>
2.5.1. L'échéance du « printemps 2007 » et au-delà	44
2.5.2. Inspections	45
<b>2.6. Mesures administratives</b>	<b>48</b>
2.6.1. Nouvel modèle de certificat médical	48
2.6.2. Accès aux documents	48
2.6.3. Catégories de données particulières : législation applicable	49
2.6.4. Demande émanant d'une juridiction en vue d'obtenir une copie du dossier médical complet d'un fonctionnaire	49
2.6.5. Conservation des informations relatives à des sanctions disciplinaires dans le cadre de la protection des données	50
2.6.6. Dispositions d'application du règlement (CE) n° 45/2001	51
2.6.7. Plaintes traitées par le médiateur européen	51
<b>2.7. Vidéosurveillance</b>	<b>51</b>
2.7.1. Lignes directrices	51
2.7.2. Contrôles préalables	52
2.7.3. Plaintes	53

2.7.4. Demandes diverses	53
<b>2.8. Eurodac</b>	<b>53</b>
<b>3. Consultation</b>	<b>54</b>
<b>3.1. Introduction</b>	<b>54</b>
<b>3.2. Cadre d'action et priorités</b>	<b>55</b>
3.2.1. Mise en œuvre de la politique de consultation	55
3.2.2. Inventaire 2008	56
3.2.3. Inventaire 2009	57
<b>3.3. Avis législatif</b>	<b>58</b>
3.3.1. Observations d'ordre général	58
3.3.2. Les avis du CEPD	59
<b>3.4. Observations</b>	<b>65</b>
<b>3.5. Interventions devant la Cour de justice</b>	<b>66</b>
<b>3.6. Autres activités</b>	<b>67</b>
3.6.1. Vie privée et communications électroniques	67
3.6.2. Dossiers passagers	67
3.6.3. Mise en œuvre du SIS et politique des frontières	68
3.6.4. Conférence sur la protection des données dans le domaine de la police et de la justice (Trèves)	68
3.6.5. RDT de l'UE	69
3.6.6. Fusion Google / DoubleClick et questions relatives à la protection des données	70
3.6.7. Participation à des groupes d'experts	71
3.6.8. Accidents maritimes	71
3.6.9. Maladies transmissibles	72
3.6.10. Le Code des douanes communautaire et le numéro d'enregistrement et d'identification des opérateurs économiques (numéro EORI)	72
<b>3.7. Nouvelles évolutions</b>	<b>72</b>
3.7.1. Interaction avec la technologie	72
3.7.2. Faits nouveaux dans les domaines politique et législatif	75
<b>4. Coopération</b>	<b>77</b>
<b>4.1. Le Groupe de l'article 29</b>	<b>77</b>
<b>4.2. Groupe « Protection des données » du Conseil</b>	<b>78</b>
<b>4.3. Supervision coordonnée d'Eurodac</b>	<b>79</b>
<b>4.4. Troisième pilier</b>	<b>80</b>
<b>4.5. Conférence européenne</b>	<b>81</b>
<b>4.6. Conférence internationale</b>	<b>81</b>
<b>4.7. L'initiative de Londres</b>	<b>82</b>
<b>4.8. Organisations internationales</b>	<b>83</b>
<b>5. Communication</b>	<b>84</b>
<b>5.1. Introduction</b>	<b>84</b>
<b>5.2. Caractéristiques de la communication</b>	<b>85</b>
<b>5.3. Discours</b>	<b>86</b>
<b>5.4. Relations avec les médias</b>	<b>89</b>
<b>5.5. Demandes d'informations</b>	<b>90</b>
<b>5.6. Visites d'étude</b>	<b>91</b>

<b>5.7. Outils d'information en ligne</b>	<b>91</b>
<b>5.8. Publications</b>	<b>93</b>
<b>5.9. Actions de sensibilisation</b>	<b>93</b>
<b>5.10. Priorités pour 2009</b>	<b>94</b>
<b>6. Administration, budget et personnel</b>	<b>95</b>
<b>6.1. Introduction</b>	<b>95</b>
<b>6.2. Budget</b>	<b>95</b>
<b>6.3. Ressources humaines</b>	<b>96</b>
6.3.1. Recrutement	96
6.3.2. Programme de stages	96
6.3.3. Programme pour les experts nationaux détachés	97
6.3.4. Organigramme	97
6.3.5. Dialogue social	97
6.3.6. Formation	97
6.3.7. Activités sociales	98
6.3.8. Protocole sur les privilèges et immunités des Communautés européennes	98
<b>6.4. Fonctions de contrôle</b>	<b>98</b>
6.4.1. Contrôle interne	98
6.4.2. Audit interne	99
6.4.3. Sécurité	99
6.4.4. Délégué à la protection des données	99
<b>6.5. Infrastructure</b>	<b>99</b>
<b>6.6. Environnement administratif</b>	<b>99</b>
6.6.1. Assistance administrative et coopération interinstitutionnelle	99
6.6.2. Règlement intérieur	100
6.6.3. Gestion des documents	101
<b>6.7. Objectifs pour 2009</b>	<b>101</b>
Annexe A — Cadre juridique	103
Annexe B — Extrait du règlement (CE) n° 45/2001	105
Annexe C — Liste des abréviations	107
Annexe D — Liste des délégués à la protection des données (DPD)	109
Annexe E — Délais de traitement des contrôles préalables par dossier et par institution	111
Annexe F — Liste des avis rendus à la suite d'un contrôle préalable	115
Annexe G — Liste des avis sur des propositions législatives	123
Annexe H — Composition du secrétariat du CEPD	125
Annexe I — Liste des accords et décisions administratifs	127



# Guide de l'utilisateur

Le lecteur trouvera, immédiatement après ce guide, l'avant-propos de M. Peter Hustinx, Contrôleur européen de la protection des données (CEPD), précédé de l'énoncé de sa mission.

**Le chapitre 1, « Bilan et perspectives »**, présente une vue générale des activités du CEPD. Il met également en lumière les résultats obtenus en 2008 et expose les principaux objectifs retenus pour 2009.

**Le chapitre 2, « Contrôle »**, décrit de façon détaillée les travaux menés pour vérifier que les institutions et organes communautaires 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 présente une analyse des contrôles préalables (quantité et contenu), des réclamations, des enquêtes, de la politique d'inspection, et des avis sur des mesures administratives traités en 2008. Il comporte également des parties consacrées au suivi électronique et à la vidéosurveillance, ainsi qu'une partie qui fait le point sur le contrôle d'Eurodac.

**Le chapitre 3, « Consultation »**, traite de l'évolution du rôle consultatif du CEPD. Il s'intéresse principalement aux avis et commentaires formulés sur des propositions législatives et documents connexes, ainsi qu'à leurs incidences dans un nombre croissant de domaines. Ce chapitre comporte aussi une analyse de thèmes horizontaux ; il présente des questions liées aux nouveautés technologiques et souligne les nouveaux développements intervenus en matière politique et sur le plan de la législation.

**Le chapitre 4, « Coopération »**, décrit le travail effectué dans des enceintes importantes telles que le Groupe de l'article 29 (Groupe sur la protection des données), 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, y compris le travail du service de presse et les activités de communication extérieure avec les médias. 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 principales évolutions intervenues au sein de l'organisation du CEPD, notamment en ce qui concerne les aspects budgétaires, la question des ressources humaines et les accords de nature administrative.

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

Le présent rapport existe également sous forme de **synthèse**, qui offre une version abrégée des principaux faits intervenus en 2008 dans le cadre des activités du CEPD.

Pour de plus amples informations sur le CEPD, nous vous invitons à consulter notre site Internet (<http://www.edps.europa.eu>), qui reste notre principal outil de communication et où vous pourrez vous inscrire pour recevoir notre bulletin d'information.

Il est possible de commander auprès d'EU Bookshop (<http://www.bookshop.europa.eu>) ou des services du CEPD des exemplaires gratuits du rapport annuel et du résumé. Nos coordonnées sont indiquées sur notre site Internet, sous la rubrique « Contact ».

# Mandat du CEPD

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

Le CEPD est chargé de :

- superviser et d'assurer le respect des dispositions du règlement (CE) n° 45/2001<sup>(1)</sup>, ainsi que d'autres actes communautaires relatifs à la protection des droits fondamentaux et des libertés lorsque les institutions et organes communautaires traitent des données à caractère personnel (« contrôle ») ;
- conseiller les institutions et organes communautaires 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 de nouveaux développements ayant une incidence sur la protection des données à caractère personnel (« consultation ») ;
- coopérer avec les autorités nationales de supervision et avec les organes de supervision 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 communautaires, 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 ;
- d'améliorer la qualité des politiques de l'UE, chaque fois que la protection effective des données personnelles est une condition essentielle au succès de ces politiques.

---

<sup>(1)</sup> Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 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 (JO L 8 du 12.1.2001, p. 1).



## Avant-propos



J'ai l'honneur de présenter au Parlement européen, au Conseil et à la Commission européenne le cinquième rapport annuel sur mes activités en qualité de contrôleur européen de la protection des données (CEPD), 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 2008, quatrième année complète d'activité depuis l'établissement du CEPD en tant que nouvelle autorité de supervision indépendante, dont la mission est de veiller à ce que, lors du traitement de 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.

Ce rapport conclut également le premier mandat du CEPD et offre l'occasion de dresser un bilan des évolutions intervenues depuis le début de ce mandat. Le contrôle indépendant prévu à l'article 286 du traité CE et confirmé en tant que principe général à l'article 8, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne, ainsi que dans le traité de Lisbonne, est une condition essentielle pour assurer dans les faits la protection des données à caractère personnel.

Les droits et libertés fondamentaux, tels que le respect de la vie privée et la protection des données à caractère personnel, ne peuvent devenir réalité que s'ils sont mis en œuvre dans la pratique, tant au sein des systèmes d'information des institutions et organes communautaires que lors de l'adoption de nouvelles règles et politiques susceptibles d'avoir une incidence sur la protection de ces données. Dans ces deux domaines, les activités du CEPD s'avèrent des stimulations utiles.

Le présent rapport montre que des progrès notables ont été réalisés, tant sur le plan de la supervision que de la consultation. Le respect des règles et principes régissant la protection des données se renforce, même s'il subsiste d'importants défis à relever. Ce qui est sans doute le plus remarquable, c'est le champ d'action actuel du CEPD si on le compare à une situation de départ où il était pour ainsi dire inexistant.

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 diverses 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.

Je tiens par ailleurs à adresser mes plus vifs remerciements d'abord à M. Joaquín Bayo Delgado, qui a été un excellent contrôleur adjoint, faisant preuve d'un grand dévouement en conjuguant sens pratique et esprit d'équipe, puis aux membres de notre personnel. Par leurs qualités exceptionnelles, ces derniers ont largement contribué à l'efficacité de notre action.

Enfin, je souhaiterais également à ce stade remercier le Parlement européen et le Conseil pour la confiance dont ils ont fait preuve en me reconduisant dans mes fonctions pour un second mandat, ainsi que pour la nomination de Giovanni Buttarelli en tant que nouveau Contrôleur adjoint.

Peter Hustinx  
*Contrôleur européen de la protection des données*



# 1. Bilan et perspectives

## 1.1. Aperçu général de 2008

Les activités que le Contrôleur européen de la protection des données (CEPD) a menées en 2008 ont été basées sur la même stratégie globale que précédemment, mais leur importance et les domaines qu'elles recouvrent ont continué de se développer. La capacité du CEPD à agir efficacement s'est également améliorée.

Le cadre juridique <sup>(2)</sup> dans lequel opère le CEPD définit un certain nombre de tâches et de compétences, qui permettent de distinguer trois fonctions principales. Ces fonctions continuent de faire office de cadre stratégique pour les activités du CEPD et sont présentées dans l'énoncé de sa mission :

- une fonction de supervision, qui consiste à superviser et assurer le respect des garanties juridiques existantes par les institutions et organes communautaires <sup>(3)</sup> 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 collaborer 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.

<sup>(2)</sup> Cf. 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)

Ces fonctions sont exposées en détail dans les chapitres 2, 3 et 4 du présent rapport annuel, qui présentent les principales activités du CEPD et les progrès réalisés en 2008. L'importance de l'information et de la communication en ce qui concerne ces activités nous a amenés à consacrer un chapitre à cette activité (cf. 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.

Les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, tels que prévus dans la Charte des droits fondamentaux de l'Union européenne et le traité de Lisbonne, sont de plus en plus importants, tant pour les particuliers et les institutions que pour la société dans son ensemble. Dans un monde qui est chaque jour davantage tributaire de l'utilisation des technologies de l'information et de la communication, ces droits sont destinés à garantir que chacun puisse y participer sans craindre que sa vie privée et ses données à caractère personnel ne soient compromis. Le respect de la vie privée et la protection des données à caractère personnel visent donc également à susciter la confiance dans les environnements technologiques avancés.

Un tel processus ne va cependant pas de soi ni ne découle des seules dispositions légales. Il nécessite que, de manière systématique, des garanties en matière de vie privée soient mises en œuvre dans la pratique, et que les règles et principes généraux soient traduits en dispositifs techniques et organisationnels concrets qui permettent de mettre en œuvre dans la réalité quotidienne les garanties voulues. Cela suppose également que ceux à qui il incombe de mener à bien ces processus soient suffisamment conscients de cet impératif et qu'ils aient à répondre de l'obtention des résultats requis dans les délais impartis.

Conscient de cet enjeu, le CEPD s'attache à favoriser au sein des institutions et organes communautaires

une « culture de la protection des données » au sein de laquelle la nécessité de respecter les règles et principes de protection des données est considérée comme allant de soi. Dans son rôle de contrôleur, le CEPD vise à encourager la responsabilité, le cas échéant en évaluant les progrès et en fixant des objectifs, mais sans être trop normatif. Il s'attache également à intégrer le respect des principes relatifs à la protection des données dans la législation et les politiques de l'UE, dans les cas où cela est justifié. Dans son rôle de conseiller, le CEPD cherche à déterminer si les propositions législatives et les nouvelles politiques ont déjà traité de ces principes comme il se devait et si elles devraient être améliorées pour répondre aux conditions requises. En coopération avec les autorités nationales de supervision et les organes de supervision relevant du troisième pilier, le CEPD s'efforce d'améliorer la cohérence sur le plan de la protection des données personnelles dans l'ensemble de l'UE.

Le CEPD a souligné d'emblée que la licéité du traitement des données personnelles 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. Le CEPD continuera d'agir selon cette ligne générale. Il est satisfait de constater un soutien de plus en plus important à cet égard.

En 2008, le contrôle préalable a continué de représenter l'essentiel des activités de supervision, le nombre d'avis rendus ayant été plus élevé que jamais. Alors que la plupart des institutions et organes réalisent des progrès notables pour ce qui est du respect du règlement (CE) n° 45/2001, la supervision porte à présent de plus en plus sur le suivi de la mise en œuvre des recommandations relatives au contrôle préalable et sur l'amélioration du respect du règlement par les agences. Le CEPD a également achevé une première série d'inspections sur place dans divers institutions et organes en vue d'évaluer le respect du règlement dans la pratique. Le nombre total de réclamations a continué d'augmenter, avec un nombre de réclamations recevables moins élevé qu'auparavant, mais des réclamations plus complexes dans l'ensemble. Des travaux supplémentaires ont également été menés en ce qui concerne la consultation sur des mesures administratives et la mise au point de lignes directrices horizontales. Le réseau des délégués à la protection des données est devenu pleinement opérationnel et demeure un instrument essentiel pour assurer l'efficacité des contrôles (cf. chapitre 2).

Le CEPD a continué, en 2008, d'améliorer son bilan en matière de consultation et a rendu des avis

sur un nombre croissant de propositions législatives. Il a élargi le champ de ses interventions à une plus grande variété de domaines et à toutes les étapes de la procédure législative, des phases les plus précoces de l'élaboration des politiques (en réagissant aux livres verts ou aux demandes de consultation informelle) aux discussions menées au Parlement et au Conseil à différents stades, y compris le stade final de la conciliation. Même si la majorité des avis du CEPD ont continué de porter sur des questions liées à l'espace de liberté, de sécurité et de justice, d'autres domaines d'action, tels que le respect de la vie privée dans le secteur des communications électroniques, l'accès du public aux documents et les soins de santé transfrontaliers ont également occupé une place importante. Le CEPD a également publié un document d'orientation sur la recherche et le développement technologique et a multiplié les interventions dans des affaires portées devant la Cour de justice (cf. chapitre 3).

La coopération avec les autorités nationales de supervision a continué d'être axée sur le rôle du groupe de protection des personnes à l'égard du traitement des données à caractère personnel (groupe de l'Article 29), ce qui a abouti à l'adoption d'un nouveau programme de travail comportant quatre thèmes stratégiques et qui a permis d'obtenir, lors de sa première année de mise en œuvre, de bons résultats. Le CEPD a également continué à mettre l'accent sur la supervision coordonnée d'Eurodac, à la fois pour le système Eurodac lui-même mais aussi compte tenu de systèmes similaires d'information à grande échelle qui devraient voir le jour dans un avenir proche. La nécessité d'une coopération étroite est très clairement apparue dans les questions relevant du troisième pilier. Enfin, la coopération dans d'autres enceintes internationales, notamment dans le cadre de « l'initiative de Londres », dont l'objectif est de mieux faire connaître la protection des données et de rendre celle-ci plus efficace, a continué à attirer l'attention (cf. chapitre 4).

L'information et la communication sont non seulement d'importants instruments en termes de visibilité, mais elles sont également indispensables au CEPD pour s'acquitter efficacement de sa mission de supervision, de consultation et de coopération. Aussi une attention particulière a-t-elle été accordée tout au long de l'année 2008 à l'amélioration des services fournis. Cela a permis d'accomplir des progrès notables, notamment en ce qui concerne le contenu et l'accessibilité du site web du CEPD. Des améliorations supplémentaires sont également en vue (cf. chapitre 5).

La gestion des ressources du CEPD, en particulier humaines et financières, s'est développée de manière significative, de la mise en place de la nouvelle institution dans les premières années de fonctionnement, puis une phase de consolidation, à une situation où des améliorations progressives ont permis de maintenir la stabilité et d'accroître l'efficacité dans différents domaines (cf. chapitre 6).

## 1.2. Résultats obtenus en 2008

Le rapport annuel 2007 exposait les principaux objectifs ci-après, qui avaient été retenus pour l'année 2008. La plupart de ces objectifs ont été totalement ou partiellement atteints.

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

Le CEPD a continué à soutenir pleinement les délégués à la protection des données (DPD) et les a encouragés à poursuivre les échanges de compétences et de bonnes pratiques. Une attention particulière a été accordée aux DPD des nouvelles agences, notamment dans le cadre d'une réunion visant à examiner les enjeux des nouvelles agences et à informer les DPD des dernières évolutions intervenues.

### • Rôle du contrôle préalable

Le CEPD a rendu un nombre record d'avis sur les notifications en vue d'un contrôle préalable, mais il reste encore du travail à accomplir pour achever le contrôle préalable des opérations de traitement en cours pour la plupart des institutions et organes. L'accent a été mis en particulier sur la mise en œuvre des recommandations du CEPD. Les résultats des contrôles préalables et de ce suivi ont été partagés avec les DPD et d'autres parties concernées.

### • Lignes directrices horizontales

Des lignes directrices ont été élaborées sur des questions pertinentes présentant un intérêt pour la plupart des institutions et organes (recrutement du personnel et traitement des données relatives à la santé, par exemple) afin, dans un premier temps, de faciliter le contrôle préalable en ce qui concerne les agences. Ces orientations seront bientôt mises à la disposition de toutes les parties intéressées. Un séminaire ayant pour but de faire connaître à d'autres acteurs de l'UE les développements intervenus dans les activités de supervision a eu lieu en décembre 2008.

### • Vérification du respect du règlement

Le CEPD a continué à vérifier le respect du règlement (CE) n° 45/2001 par l'ensemble des institutions et organes, et fera rapport des progrès accomplis en la matière d'ici la mi-2009. Outre cette évaluation de nature générale, une première

série d'inspections a été réalisée dans divers organes et institutions afin de vérifier le respect de certains points particuliers. Une politique générale d'inspection sera également publiée sur le site web du CEPD en 2009.

### • Systèmes à grande échelle

Le CEPD a continué à mettre en place une supervision coordonnée d'Eurodac avec les autorités de contrôle nationales et à mettre en œuvre le programme de travail adopté à cet effet. Les résultats de ces activités conjointes seront disponibles en 2009. Le CEPD a également pris les premières mesures concernant d'autres systèmes à grande échelle, tels que le SIS II et le VIS.

### • Avis sur les propositions législatives

Le CEPD a rendu un nombre record d'avis et d'observations sur des propositions législatives ou des documents connexes, couvrant un domaine plus large qu'auparavant. Il a apporté une contribution appropriée du premier au tout dernier stade de la procédure législative. L'inventaire systématique des priorités en la matière a fait l'objet d'un suivi tout au long de l'année et a donné lieu, le cas échéant, à des mises à jour.

### • Traité de Lisbonne

L'incidence du traité de Lisbonne a fait l'objet d'une analyse approfondie, mais son entrée en vigueur est subordonnée à sa ratification définitive par quelques États membres. L'analyse a souligné que le traité est susceptible d'avoir une grande incidence, tant pour des raisons institutionnelles que pour des raisons de fond, et qu'il offre des possibilités évidentes d'amélioration en matière de protection des données.

### • Informations en ligne

Les informations disponibles sur le site web du CEPD ont été améliorées grâce à l'actualisation et à l'enrichissement de son contenu, et l'accès au site a été amélioré. D'autres améliorations devraient être apportées en 2009, notamment en ce qui concerne la lettre d'information électronique.

### • Règlement intérieur

L'élaboration d'un règlement intérieur s'appliquant aux différentes fonctions et activités du CEPD a bien progressé, de même que la mise au point de manuels internes concernant les activités les plus importantes. Les résultats seront disponibles sur le site web du CEPD en 2009, assortis d'outils pratiques destinés aux parties intéressées.

### • Gestion des ressources

La gestion des ressources financières et humaines a été consolidée et développée, et d'autres procédures

internes ont été améliorées. La fonctionnalité et l'efficacité des mécanismes de contrôle interne ont également été améliorées.

### 1.3. Objectifs en 2009

Cette partie du rapport annuel s'attachait les précédentes années à envisager l'avenir. Pour cet exercice-ci, il convient cependant de s'attendre à la fois à une continuité et à des changements. L'année 2009, la première du nouveau mandat du CEPD et du renouvellement partiel de l'institution, offre ainsi l'opportunité d'évaluer la nécessité éventuelle d'ajustements. Elle sera donc mise à profit pour procéder à une évaluation stratégique des rôles et des fonctions du CEPD et fixer les grandes lignes d'action pour les quatre prochaines années. Cette réflexion coïncidera avec des éléments nouveaux dans notre environnement extérieur, tels que les défis résultant d'une nouvelle législature européenne, d'une nouvelle Commission européenne, de l'éventuelle entrée en vigueur du traité de Lisbonne, ainsi que de nouvelles politiques et de nouveaux cadres à long terme et de leurs incidences combinées sur la protection des données. Le CEPD entend adopter une position claire dans ce contexte et en rendra compte dans les conclusions de son prochain rapport annuel.

Les principaux objectifs ci-après ont été retenus pour 2009, sans préjudice de l'issue de ce processus de réflexion. Les résultats obtenus à cet égard seront consignés dans le rapport qui sera présenté l'année prochaine.

- **Soutien au réseau des DPD**

Le CEPD continuera à soutenir pleinement les délégués à la protection des données (DPD), en particulier ceux des nouvelles agences, et les encouragera à poursuivre leurs échanges de compétences et de bonnes pratiques, afin d'accroître leur efficacité.

- **Rôle du contrôle préalable**

Le CEPD a l'intention d'achever le contrôle préalable des opérations de traitement en cours pour la plupart des institutions et organes, et de mettre de plus en plus l'accent sur la mise en œuvre de ses recommandations. Une attention particulière sera accordée au contrôle préalable des opérations de traitement communes à la plupart des agences.

- **Lignes directrices horizontales**

Le CEPD continuera à élaborer des lignes directrices sur des questions présentant un intérêt commun pour la plupart des institutions et organes, et à les diffuser largement. Des orientations seront publiées

sur la vidéosurveillance afin d'attirer également l'attention sur des situations qui présentent des risques particuliers.

- **Traitement des réclamations**

Le CEPD publiera un cadre relatif au traitement des réclamations afin d'informer toutes les parties concernées des procédures pertinentes, notamment des critères permettant de déterminer s'il convient ou non d'ouvrir une enquête sur les réclamations qui lui sont présentées.

- **Politique d'inspection**

Le CEPD continuera à vérifier le respect du règlement (CE) n° 45/2001 par le biais de différents types de contrôles concernant tous les organes et institutions, et effectuera de plus en plus d'inspections sur le terrain. Des lignes directrices sur les procédures applicables en la matière seront publiées.

- **Étendue des consultations**

Le CEPD continuera à rendre des avis ou à formuler des observations en temps utile sur les nouvelles propositions législatives en se fondant sur un inventaire, établi de façon systématique, des priorités et des sujets pertinents. Il continuera à en assurer un suivi approprié.

- **Programme de Stockholm**

Le CEPD entend accorder une attention particulière à la préparation du nouveau programme d'action de cinq ans relatif à l'espace de liberté, de sécurité et de justice, en vue de son adoption par le Conseil européen à la fin de 2009. La nécessité de garanties efficaces pour la protection des données sera mise en avant en tant que condition essentielle.

- **Activités d'information**

Le CEPD continuera d'améliorer la qualité et l'efficacité des outils d'information en ligne (site web et lettre d'information électronique) et procédera à une évaluation et, si nécessaire, à une actualisation de ses autres activités d'information.

- **Règlement intérieur**

Le CEPD adoptera et publiera un règlement intérieur, qui confirmera ou précisera les pratiques actuelles quant à ses différents rôles et activités. Des outils pratiques destinés aux parties intéressées seront disponibles sur le site web.

- **Gestion des ressources**

Le CEPD consolidera et continuera de développer les activités liées aux ressources financières et humaines, et il améliorera les méthodes de travail internes. Une attention particulière sera accordée au recrutement de personnel à long terme, au besoin d'espaces de bureaux supplémentaires et à l'élaboration d'un système de gestion des dossiers.

## 2. Supervision

### 2.1. Introduction

La mission du Contrôleur européen de la protection des données (CEPD) consiste à surveiller, de manière indépendante, les traitements de données à caractère personnel effectués par les institutions et 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 supervision.

Cette année encore, le contrôle préalable des opérations de traitement a constitué l'essentiel des activités de supervision, dans le prolongement des notifications reçues après ce que l'on appelle l'exercice « printemps 2007 ». 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. Le CEPD a effectué un contrôle préalable des opérations de traitement existantes, ainsi que de celles qui sont planifiées, dans la plupart des catégories pertinentes. 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 réclamations, la réalisation d'enquêtes ou d'inspections, et les conseils concernant des mesures administratives.

Pour ce qui est des compétences qui lui sont confiées, le CEPD n'a ordonné aucune mesure et n'a émis aucun avertissement ni interdiction, pas plus en 2008 qu'au cours des années précédentes, les



M. Joaquín Bayo Delgado, Contrôleur adjoint – responsable de l'équipe de supervision

responsables du traitement ayant mis en œuvre ses recommandations ou exprimé leur intention de le faire en prenant les mesures nécessaires à cette fin. La rapidité des réactions varie selon les cas. Le CEPD assure un suivi systématique de ses recommandations.

### 2.2. Délégués à la protection des données

Le règlement prévoit qu'au moins une personne doit être désignée comme délégué à la protection des données (DPD) (article 24, paragraphe 1). Certaines institutions ont associé à ce délégué un assistant ou un adjoint. La Commission a également nommé un DPD pour l'Office européen de lutte antifraude (l'OLAF, une direction générale de la Commission) et, dans chacune des autres directions générales, un « coordinateur de la protection des données » chargé de coordonner tous les aspects de la protection des données au sein de la DG concernée.

Depuis plusieurs années, les DPD se rencontrent régulièrement afin d'échanger leurs expériences et d'examiner des questions horizontales. Ce réseau



Les délégués à la protection des données lors de leur 21<sup>ème</sup> réunion (Bruxelles, 26 juin 2008).

informel a fait la preuve de son efficacité en termes de collaboration, ce qui a continué d'être le cas en 2007.

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

Le CEPD a assisté à une partie de chacune des réunions que les DPD ont tenues en 2008 : à Luxembourg en février (Parlement européen), à Bruxelles en juin (Comité des régions et Comité économique et social européen) et à Strasbourg en octobre (Commission européenne). Ces réunions ont permis au CEPD d'informer les DPD sur les derniers développements intervenus dans le cadre de sa mission et de discuter des questions d'intérêt commun. Le CEPD a mis à profit ces enceintes pour expliquer et passer en revue la procédure des contrôles préalables et certaines des principales questions qui découlent du travail mené dans ce cadre. Lors de chaque réunion, les DPD ont été informés des progrès réalisés dans le domaine des notifications en vue d'un contrôle préalable.

Les réunions tenues entre le CEPD et les DPD ont également permis au premier d'informer les seconds

sur les derniers développements intervenus dans le cadre de l'exercice « printemps 2007 » et de son suivi, notamment dans le domaine des inspections (cf. point 2.5.1. « L'échéance du « printemps 2007 » et au-delà »). Ces réunions ont donné l'occasion à certains des DPD et au CEPD d'échanger des informations au sujet des initiatives prises lors de la Journée européenne de la protection des données (28 janvier). Le CEPD a également effectué des présentations sur l'état des projets pilotes dans le domaine des contrôles préalables, les transferts de données médicales aux juridictions nationales et les clauses contractuelles devant être insérées dans les appels d'offres entre les institutions de l'UE et les sous-traitants de données à caractère personnel.

Une réunion a également eu lieu en juin dans les bureaux du CEPD, au cours de laquelle les DPD des agences de l'UE ont examiné des questions particulières de fond et de procédure en rapport avec ces agences. La nouvelle procédure de contrôle préalable *a posteriori* des agences (cf. point 2.3.2. sur la procédure) a également été examinée dans ce cadre. Les services du CEPD ont aussi effectué à cette occasion une présentation sur les principales procédures pour lesquelles le CEPD a conclu qu'elles tombent en dehors du champ d'application de l'article 27 du règlement et qu'elles ne sont donc pas soumises au contrôle préalable.

Le groupe de travail sur les délais de conservation des données, leur verrouillage et leur effacement a

organisé trois ateliers en 2008, auxquels ont pris part le Contrôleur adjoint et deux membres du personnel. Des experts informatiques issus des institutions participant aux ateliers ont été invités à se joindre aux discussions et à faire part de leurs observations. Des projets de scénarios donnant un aperçu des principales questions leur ont été soumis pour discussion. À l'issue des travaux qu'il a menés, le groupe de travail a établi un document de travail, qui a été communiqué aux DPD pour qu'il puisse ensuite être consulté par les services informatiques.

## 2.3. Contrôles préalables

### 2.3.1. Base juridique

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

L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 dispose que tous « les traitements susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées du fait de leur nature, de leur objet 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.

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

L'article 27, paragraphe 2, du règlement énumère un certain nombre de traitements susceptibles de présenter des risques particuliers au regard des droits et des 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 (à savoir des mesures adoptées dans le cadre d'une procédure judiciaire) ;
- b) les opérations de traitement destinées à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement ;

- c) les opérations de traitement permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire 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<sup>(4)</sup> 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 (cf. 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 civils, mais lorsque ceux-ci coïncident avec des périodes de vacances, il s'agit de jours ouvrables – 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 2008, le mois d'août a été exclu des calculs, tant pour les institutions/organes que pour le CEPD.

<sup>(4)</sup> Cf. rapport annuel 2005, point 2.3.1.



L'équipe de supervision en réunion.

### **Procédure applicable aux contrôles préalables *a posteriori* dans les agences**

Le CEPD a mis en place une nouvelle procédure applicable aux contrôles préalables *a posteriori* dans les agences. Étant donné que les procédures standard sont souvent identiques dans la plupart des agences de l'UE et sont fondées sur des décisions de la Commission, l'idée est de rassembler les notifications portant sur un thème similaire et soit de rendre un avis collectif (pour plusieurs agences), soit de réaliser un « mini-contrôle préalable » traitant des seules particularités d'une agence. Pour aider les agences à remplir leurs notifications, le CEPD présentera un résumé des principaux points et conclusions sur le thème concerné en s'inspirant des avis rendus sur la notification en vue d'un contrôle préalable (notamment pour la Commission). Le DPD soumettra ensuite une notification au sens de l'article 27, assortie d'une note soulignant des aspects particuliers au regard de la position du CEPD dans ce domaine (particularités du traitement au sein de l'agence, questions posant problème, etc.). Cette procédure a été lancée en octobre 2008 avec comme premier thème le recrutement.

### **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 être accessible au public pour consultation.

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 rendu son avis, celui-ci est rendu public. Tous les avis, ainsi qu'un résumé du dossier concerné, sont disponibles sur le site Internet du CEPD, qui comprend désormais le registre, de sorte que les notifications sont également disponibles.

### **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 et des conclusions.

L'analyse juridique consiste, en premier lieu, 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 et 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.

Un manuel garantit, 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 peut 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 qui présentent des risques particuliers.

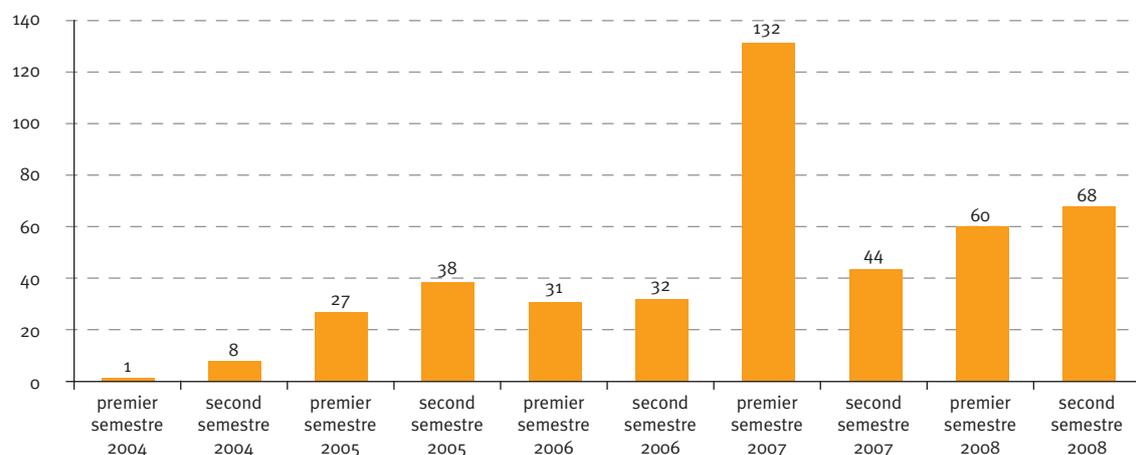
En 2004 et en 2005, certaines catégories ont été recensées dans la plupart des institutions et organes et il a été estimé qu'elles se prêtaient à un contrôle plus systématique (dossiers médicaux et autres dossiers contenant des données relatives à la santé, évaluation du personnel, y compris le recrutement du personnel, procédures disciplinaires, services sociaux et contrôle des communications électroniques). Depuis le printemps 2007, ces catégories ne s'appliquent plus à la définition de priorités et sont uniquement 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. Les cas de contrôle préalable concernent de moins en moins ces domaines mais des traitements permettant des interconnexions non prévues en vertu de la législation (article 27, paragraphe 2, point c), du règlement).

**2.3.3. Évaluation quantitative**

**Notifications de contrôle préalable**

Comme indiqué dans les précédents rapports annuels, le CEPD a constamment encouragé les délégués à la protection des données à lui adresser davantage de notifications en vue d'un contrôle préalable.

**Notifications adressées au CEPD**



L'échéance fixée au printemps 2007 (voir le rapport annuel 2007) a incité les institutions et les organes communautaires à redoubler d'efforts en vue de respecter pleinement leur obligation de notification, ce qui a eu pour effet une nette augmentation du nombre de notifications. En 2008, le nombre de notifications s'est nettement ralenti, mais comme le montrent les chiffres (voir le graphique ci-dessous), le nombre d'avis rendus est plus élevé qu'en 2007, conséquence directe du printemps 2007.

### Avis rendus en 2008 sur des cas de contrôle préalable

En 2008, **105 avis** <sup>(2)</sup> ont été rendus sur des notifications adressées en vue d'un contrôle préalable.

Conseil de l'Union européenne	16 dossiers
Commission européenne	34 dossiers
Banque centrale européenne (BCE)	1 dossier
Cour de justice	1 dossier
Banque européenne d'investissement (BEI)	2 dossiers
Parlement européen	9 dossiers AESM
Centre de traduction des organes de l'Union européenne (CdT)	1 dossier
Office européen de sélection du personnel (EPSO) <sup>(1)</sup>	1 dossier
Cour des comptes européenne	4 dossiers
Comité des régions (CdR)	1 dossier
Comité économique et social européen	3 dossiers
C.E.S./CdR	2 dossiers
Médiateur européen	1 dossier
Office de l'harmonisation dans le marché intérieur (OHMI)	4 dossiers
Office européen de lutte antifraude (OLAF)	4 dossiers
Office communautaire des variétés végétales (OCVV)	2 dossiers
Centre européen pour le développement de la formation professionnelle (Cedefop)	3 dossiers
Autorité européenne de sécurité des aliments (EFSA)	2 dossiers
Observatoire européen des drogues et des toxicomanies (OEDT)	5 dossiers
Agence européenne des médicaments (EMA)	5 dossiers
Agence européenne pour la sécurité maritime (AESM)	3 dossiers
Agence des droits fondamentaux de l'Union européenne	1 dossier

(1) L'EPSO fait appel au délégué de la Commission européenne.

(2) Le CEPD a reçu 109 notifications mais pour des raisons pratiques, certains cas ont été traités conjointement, vu le lien existant entre eux. C'est pourquoi 105 avis ont été rendus pour 109 notifications.

Par rapport à 2007, ces 109 dossiers représentent une augmentation de 8 % de la charge de travail pour les contrôles préalables.

Sur les 109 dossiers de contrôle préalable (105 avis), 18 étaient des cas de contrôle préalable proprement dit, c'est-à-dire que les institutions concernées (un pour chacune des institutions et organes suivants : Cour des comptes, Cedefop, Comité économique et social européen, Comité des régions, Agence des droits fondamentaux, et OHMI, deux pour le Parlement, trois pour l'OLAF et quatre pour le Conseil et la Commission) ont suivi la procédure relative au contrôle préalable avant la mise en œuvre de l'opération de traitement.

Ces 18 cas de contrôle préalable proprement dits ont donné lieu à 16 avis car deux dossiers du Parlement européen avaient un lien, l'un avec l'Agence des droits fondamentaux et l'autre avec le Conseil (sélection des membres du comité scientifique de l'Agence des droits fondamentaux et sélection du CEPD et du Contrôleur adjoint).

Les autres avis concernaient les questions suivantes :

- horaire flexible/flexitime,
- appels d'offres (deux dossiers) ;
- système de sécurité de la télévision en circuit fermé (CCTV) (voir également le point 2.7) ;
- sélection de candidats au poste de CEPD et de Contrôleur adjoint (Commission) ;
- interconnexions non prévues en vertu de la législation (article 27, paragraphe 2, point c), du règlement) entre des données traitées pour des finalités différentes (interface flexitime Persona Grata) ;
- contrôle d'identité et contrôle de l'accès (deux dossiers) ;
- contrôle de l'utilisation d'Internet ;
- projet pilote relatif au contrôle de la production individuelle ;
- système de gestion de la qualité ;
- enquêtes administratives et mesures disciplinaires ; et
- coordination de l'assistance médicale, psychosociale et administrative (Compas) (voir également le point 2.3.5).

Les autres avis étaient des contrôles préalables « *a posteriori* ».

Outre les notifications sur lesquelles un avis a été rendu, le CEPD a traité 13 dossiers qui ont été considérés comme ne devant pas faire l'objet d'un contrôle préalable. Le CEPD constate avec satisfaction une diminution du nombre de dossiers

considérés comme ne devant pas faire l'objet d'un contrôle préalable. Cela s'explique certainement en partie par l'échéance fixée au printemps 2007 qui a sensibilisé les délégués à la protection des données et abouti à une meilleure évaluation avant l'envoi des notifications. L'analyse de ces 13 dossiers est détaillée au point 2.3.7.

Neuf notifications ont été retirées, dont un dossier de la BEI sur le traitement des données concernant des « personnes politiquement exposées » (analyse présentée au point 2.3.7 avec les dossiers considérés comme ne devant pas faire l'objet d'un contrôle préalable). Pour la première fois, le CEPD a décidé de proposer que certaines notifications soient retirées car elles concernaient d'anciens traitements sur le point d'être remplacés par de nouveaux ou car elles ne contenaient pas suffisamment d'informations, ce qui rendait leur traitement impossible faute d'une bonne connaissance des faits ou de la procédure.

Le CEPD encourage les délégués à la protection des données à formuler leurs notifications le plus clairement possible, ce qui a pour effet immédiat de réduire la période de suspension nécessaire à l'institution ou à l'organe pour répondre aux demandes d'information émanant du CEPD. Le CEPD a l'intention d'élaborer un formulaire de notification étayée à l'intention de tous les délégués à la protection des données pour les informer avec précision, ainsi que les responsables du traitement, des informations requises.

### Analyse par institution et organe

À la suite de l'exercice du printemps 2007, les institutions et organes communautaires ont réalisé des progrès en ce qui concerne le respect du règlement. La plupart des institutions et organes ont notifié des opérations de traitement susceptibles de présenter des risques spécifiques.

La Commission européenne a réalisé d'importants progrès dans ce domaine, avec un nombre non négligeable de notifications émanant du Centre commun de recherche de la Commission (CCR). Le Conseil et les deux Comités ont également nettement progressé. La Banque européenne d'investissement et la Banque centrale européenne ont adressé moins de notifications mais elles auront davantage d'occasions de le faire du fait des nouvelles questions à traiter.

Parmi les agences européennes, le Cedefop, l'OEDT, l'EMEA et l'AESM se sont montrées très actives en matière de notification d'opérations de traitement. D'autres agences ont commencé à notifier des

opérations de traitement. En 2009, il ne fait aucun doute que le nombre de notifications émanant des agences va nettement augmenter. Le CEPD a commencé à formuler des orientations sur la manière d'effectuer une notification selon une nouvelle procédure concernant les contrôles préalables effectués *a posteriori* sur la base des lignes directrices élaborées par le CEPD, notamment dans le domaine du recrutement et des données relatives à la santé.

### Analyse par catégorie

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

Première catégorie (dossiers médicaux)	28 dossiers
Deuxième catégorie (évaluation du personnel)	53 dossiers
Troisième catégorie (procédures disciplinaires)	6 dossiers
Quatrième catégorie (services sociaux)	0 dossier
Cinquième catégorie (suivi électronique)	4 dossiers
Autres domaines	14 dossiers

**La première catégorie** comprend notamment le dossier médical à proprement parler et son contenu, les accidents du travail, les absences pour maladie, la procédure d'invalidité, les crèches, les régimes d'assurance maladie, les procédures liées aux indemnités, la dosimétrie des rayonnements et trois dossiers concernant des données relatives à la santé. Cette catégorie a nettement augmenté par rapport à l'année précédente. Parmi les 28 dossiers, 17 émanent des différents sites des CCR. Ce nombre croissant a donné au CEPD l'occasion de donner des conseils sur les procédures liées aux données relatives à la santé dans les principales institutions.

**La catégorie** la plus représentée reste la **deuxième**, relative à l'évaluation du personnel (53 avis sur 105). Vingt-trois dossiers concernaient le recrutement (de fonctionnaires, d'agents contractuels et temporaires, de stagiaires, d'experts, de membres de comités scientifiques, du CEPD et de l'assistant du CEPD). Les autres dossiers concernaient notamment l'évaluation, les promotions, les procédures de certification et d'attestation, le flexitime et la retraite anticipée.

Pour ce qui est de la **troisième catégorie** concernant les infractions et les suspensions, on a pu constater une nette diminution du nombre de dossiers (six avis contre dix-huit en 2007). Seul un avis a été rendu sur des procédures disciplinaires, la plupart des institutions ayant déjà notifié ce type de dossiers au cours des années précédentes. Un autre avis a été rendu sur

les enquêtes de sécurité (voir le point 2.3.4), deux avis dans le domaine du harcèlement et deux autres dans d'autres domaines.

En ce qui concerne la **quatrième catégorie** concernant les services sociaux, le CEPD n'a reçu aucune notification, ce qui peut se comprendre car cette catégorie a déjà fait l'objet de contrôles préalables pour les plus grandes institutions, et la plupart des agences ne sont généralement pas en mesure de proposer ce type de service à leur personnel.

Pour ce qui est de la **cinquième catégorie** (suivi électronique), seuls quatre avis ont été rendus. Étant donné que la plupart de ces notifications concernaient un traitement de données relatives à la facturation et à la gestion du trafic, le CEPD a estimé que 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 en vertu de l'article 27. Il convient toutefois de souligner l'avis adressé à la Cour des comptes qui concerne le contrôle des communications (dossier 2008-284, voir l'analyse au point 2.3.4).

En ce qui concerne les notifications ne relevant pas de ces catégories, le CEPD a continué de rendre des avis dans les domaines suivants :

- appels d'offres ;
- système de contrôle d'accès en cas d'utilisation d'un système de correspondance biométrique ;
- télévision en circuit fermé (un avis qui est un cas de contrôle préalable proprement dit – voir le point 2.7) ;
- interconnexion de bases de données (dossier 2008-324 – Persona Grata – Conseil – voir le point 2.3.5) ;
- questions diverses, comme l'accréditation ou le témoignage en justice.

### Respect des délais de paiement

Les quatre graphiques de l'annexe E du présent rapport illustrent le temps consacré au traitement des avis relatifs aux contrôles préalable par le CEPD et les institutions et organes communautaires. Ils fournissent des informations détaillées sur le nombre de jours 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 nécessaires à l'élaboration d'un avis du CEPD* : Le nombre de jours nécessaires à l'élaboration d'un avis a diminué de plus de deux jours

par rapport à 2007, soit 55 jours en moyenne par avis en 2008. Ceci est très satisfaisant compte tenu de l'augmentation du nombre et de la complexité des notifications transmises au CEPD.

*Nombre de jours de travail dans le cadre d'une prolongation du délai prévu pour l'avis du CEPD* <sup>(6)</sup> : Le CEPD a demandé une prolongation de délai pour neuf dossiers. Bien qu'il soit possible de demander une prolongation de deux mois (article 27, paragraphe 4, du règlement), la prolongation demandée est généralement d'un mois. Dans la pratique toutefois, tous les avis ont été adoptés dans ce délai d'un mois, et, pour la majorité d'entre eux, dans un délai beaucoup plus court.

*Nombre de jours de suspension* <sup>(7)</sup> : Le nombre de jours de suspension a augmenté en 2008 (122 jours en moyenne par dossier) par rapport à 2007 (75 jours en moyenne par dossier).

Compte tenu de ce que la moyenne était de 30 jours par dossier en 2005 et de 73 jours en 2006, le CEPD est préoccupé par le temps que mettent les institutions et organes à transmettre des informations complémentaires. De fait, pour certains dossiers, la suspension a atteint 524 jours dans l'attente d'informations complémentaires. Le CEPD trouve cette situation inacceptable et il rappelle 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 et organe* : En 2008, les tableaux montrent une augmentation inquiétante du nombre de jours de suspension pour presque toutes les institutions et organes. À l'exception du Parlement européen et de l'EFSA, qui ont réussi à faire baisser leur moyenne, le nombre de jours de suspension a considérablement augmenté pour toutes les autres institutions et organes. C'est le cas notamment de la BEI, du Conseil, de la Commission, de la Cour des comptes, de la Cour de justice et des agences.

Le CEPD reconnaît que la majeure partie du temps de suspension est imputable au responsable du traitement. Néanmoins, les délégués à la protection des données devraient accorder plus d'attention à ces

<sup>(6)</sup> Selon l'article 27, paragraphe 4, le CEPD peut, lorsque la complexité du dossier le rend nécessaire, décider de prolonger de deux mois le délai dans lequel il doit rendre son avis.

<sup>(7)</sup> Depuis la mi-2006, cette période comprend le délai de sept ou dix 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 2008, le mois d'août n'est pas compris dans le calcul.

délais. C'est en effet à eux qu'incombe la responsabilité finale en ce qui concerne la notification et les informations complémentaires, même si, pour d'éventuelles raisons pratiques, les demandes peuvent être adressées directement au responsable du traitement, avec copie au délégué.

**Notifications adressées en vue d'un contrôle préalable reçues avant le 1<sup>er</sup> janvier 2009 et en cours d'examen**

À la fin de 2008, 69 cas de contrôle préalable étaient en cours de traitement. Parmi ceux-ci, une notification avait été adressée en 2006, 11 en 2007 et 55 en 2008.

**Analyse par institution et organe**

Parlement	7 dossiers
Conseil de l'Union européenne	6 dossiers
Commission européenne	33 dossiers
CESE et CdR	1 dossier
CESE	4 dossiers
CdR	3 dossiers
BEI	2 dossiers
ECA	2 dossiers
Cour de justice	1 dossier
Cedefop	1 dossier
OCVV	1 dossier
EFSA	1 dossier
EMEA	3 dossiers
FEF	1 dossier
FRA	2 dossiers
OHMI	1 dossier

**Analyse par catégorie**

Les cas de contrôle préalable notifiés en cours au 1<sup>er</sup> janvier 2009 se répartissent comme suit, par catégorie :

Première catégorie (dossiers médicaux)	20 dossiers
Deuxième catégorie (évaluation du personnel)	26 dossiers
Troisième catégorie (procédures disciplinaires)	4 dossiers
Quatrième catégorie (services sociaux)	0 dossier
Cinquième catégorie (suivi électronique)	3 dossiers
Autres domaines	16 dossiers

**2.3.4. Principales questions soulevées par les dossiers examinés a posteriori**

**Données relatives à la santé**

Le CEPD a rendu divers avis sur le traitement des données à caractère personnel dans le domaine des absences pour raison médicale (maladie ou accident). Le CEPD a notamment recommandé que les données recueillies par le service médical du Parlement européen afin de justifier une absence pour raison médicale ne puissent être utilisées à d'autres fins (notamment à des fins de prévention) sans le consentement libre et informé de la personne concernée (dossier 2007-688) Le CEPD a également estimé dans ce dossier que les données ne pouvaient être conservées plus de 12 ans pour ce qui concerne les personnes qui ont quitté l'institution.

Le CEPD a également procédé au contrôle préalable du traitement des données à caractère personnel relatives aux absences pour raisons médicales au Conseil dans les dossiers 2008-271 et 2008-283. Les recommandations portaient essentiellement sur la conservation des données par le médecin contrôleur pendant une durée de 30 ans et le CEPD a invité le médecin contrôleur à reconsidérer cette durée à la lumière des finalités du traitement.

Le CEPD a rendu un avis de contrôle préalable relatif au logiciel PowerLab utilisé par le Centre commun de recherche (CCR) de la Commission européenne (dossier 2007-649).

PowerLab est un logiciel utilisé pour la gestion du cycle de travail des laboratoires cliniques et radio-toxicologiques du CCR. Il est utilisé en relation



Les institutions et agences communautaires traitent des données relatives à la santé.

avec les analyses effectuées dans le cadre des visites médicales d'embauche, des visites médicales annuelles ainsi que d'autres visites médicales liées aux risques professionnels spécifiques. Il comprend également la production et/ou la conservation des rapports d'examens correspondants.

Les principales recommandations formulées dans l'avis de contrôle préalable relatif à PowerLab portent sur :

- la nécessité que tout le personnel de laboratoire respecte l'obligation de secret professionnel ;
- l'obligation de ne pas utiliser les données reçues à d'autres fins que celles pour lesquelles elles ont été transmises ; et
- la nécessité de fournir des renseignements complets.

#### Accréditation des journalistes

Le CEPD a rendu un avis sur la notification d'un contrôle préalable concernant l'accréditation des journalistes participant aux réunions du Conseil européen (dossier 2004-259). La finalité du traitement est de permettre au Bureau de sécurité du Conseil d'effectuer une appréciation en termes de sécurité des membres de la presse participant aux sommets. Les personnes enregistrées peuvent, le cas échéant, recevoir un badge leur octroyant l'accès au périmètre de sécurité établi autour du bâtiment dans lequel le sommet a lieu.

La gestion des informations concernant les journalistes à des fins de contrôle de sécurité est faite de la

manière suivante : les informations sont collectées depuis un formulaire sur un site sécurisé (HTTPS) sur l'intranet du Conseil.

L'administrateur du système crée alors automatiquement les listes de demande de « screening » qui sont envoyées aux différents services de sécurité (Autorité Nationale de Sécurité – ANS belge ou ANS de la présidence). Les listes créées à cet effet mentionnent le nom, le prénom, la date de naissance et la nationalité de la personne. Les résultats sont communiqués aux responsables du système au Bureau de sécurité d'abord par téléphone (par souci d'efficacité) puis par courrier officiel. Ils se limitent au screening « positif » ou « négatif ». Néanmoins, en vertu de la décision du Secrétaire général du Conseil n° 198/03, le directeur du Bureau de sécurité du Conseil peut en décider autrement, de façon exceptionnelle, durant la tenue d'un sommet (par exemple, en cas de comportement inadéquat).

La période initiale de conservation est de cinq ans mais le Conseil a manifesté la volonté de conserver les données pendant 30 ans. À cet égard, le CEPD a recommandé qu'une durée proportionnelle soit fixée, eu égard à la finalité du traitement. Le CEPD a également demandé que la mention « Il importe de remarquer que les candidats donnent ces données sur base volontaire et que nul n'est obligé de les donner » ne figure pas dans la note d'information car, la plupart du temps, les journalistes demandent une accréditation dans le cadre de leur travail et l'on peut donc s'interroger sur la valeur de leur consentement au sens de l'article 2, point h), du règlement.

Un avis sur la notification d'un contrôle préalable a également été rendu sur l'accréditation du personnel des entreprises externes aux réunions du Conseil européen (dossier 2007-46). Le CEPD est parvenu aux mêmes conclusions.

Service de gestion de l'identité Le CEPD a rendu un avis (dossier 2007-349) sur une notification en vue d'un contrôle préalable concernant le traitement des données à caractère personnel que la DG Informatique de la Commission européenne effectue dans le cadre du service de gestion de l'identité.

Ce service est essentiellement utilisé pour la gestion des utilisateurs et de leurs droits dans le cadre des



L'accréditation des journalistes et des sociétés extérieures visant à leur permettre d'avoir accès aux sommets du Conseil a fait l'objet d'un contrôle préalable de la part du CEPD.

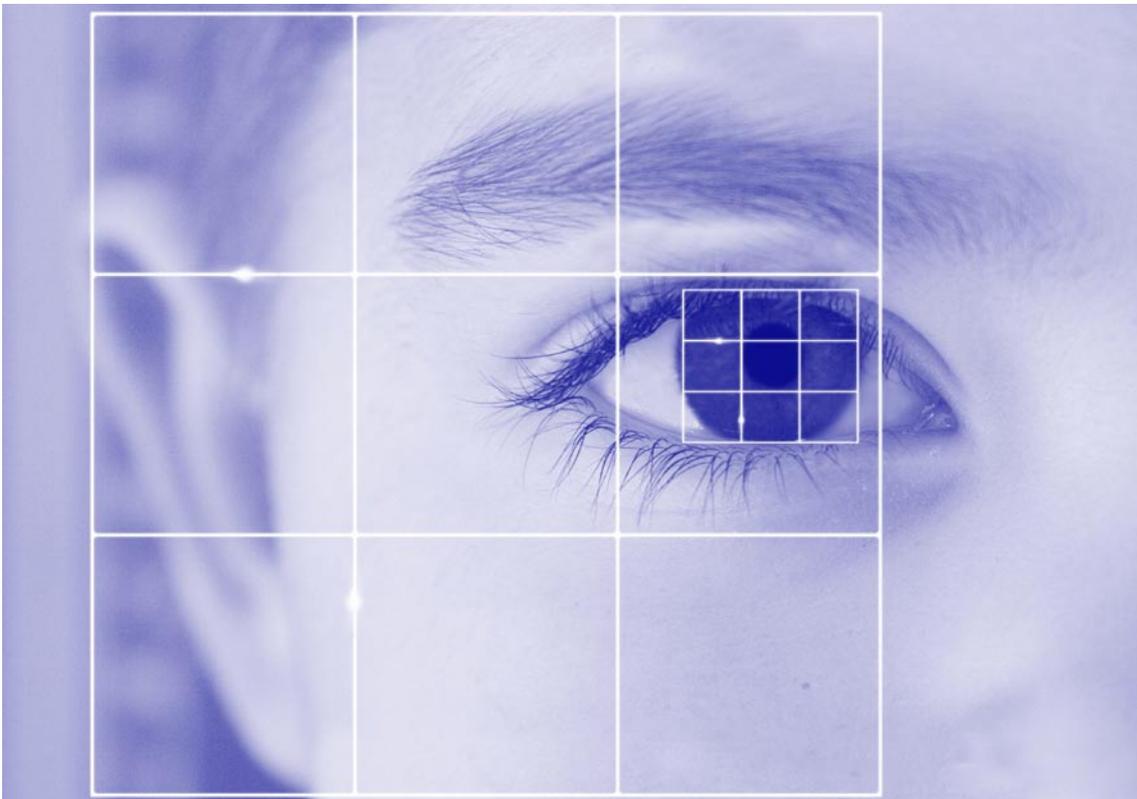
services d'information. Le SGI facilite notamment l'authentification et le contrôle d'accès des utilisateurs à différents services d'information de la Commission européenne, qui sont gérés par différentes directions générales. Ce faisant, le SGI personnalise les interfaces utilisateurs suivant les caractéristiques propres à chaque utilisateur. Le SGI est destiné au personnel de la Commission ainsi qu'au personnel d'autres organisations et aux citoyens.

Le CEPD a conclu dans son avis que la Commission a respecté le règlement (CE) n° 45/2001. Néanmoins, le CEPD a formulé des recommandations concernant la licéité du traitement et suggéré la nécessité d'obtenir le consentement de l'utilisateur sur le traitement de ses données à caractère personnel par le SGI à des fins de personnalisation (de façon interactive et sur l'écran par exemple, à l'aide d'une fenêtre contextuelle). Le CEPD a également recommandé de réduire la période de conservation des fichiers-journaux, conformément à l'article 37, paragraphe 2, du règlement. Le CEPD a reconnu que le SGI effectue des mises à jour régulières et automatiques des informations concernant le personnel obtenues

à partir de bases de données des ressources humaines et qu'il garantit donc l'exactitude des données relatives aux membres du personnel. Toutefois, il semble qu'il n'existe pas de système similaire pour les informations relatives aux utilisateurs externes. Il se peut que ces utilisateurs aient été inscrits par un tiers tel que leur employeur, ce qui augmente le risque d'inexactitude de ces informations. Le CEPD a donc souligné qu'il est important de mettre en place un système garantissant l'exactitude des informations à caractère personnel concernant les membres du personnel d'une entreprise externe à la Commission qui ont été inscrits au SGI par un tiers, comme leur employeur.

### Contrôle de l'accès

Le CEPD a rendu un avis sur une notification en vue d'un contrôle préalable concernant la mise en place d'un système de contrôle d'accès à reconnaissance de l'iris pour les membres du personnel de la Banque centrale européenne (BCE), ainsi que pour les personnes extérieures pénétrant dans les zones hautement sécurisées de l'institution (dossier 2007-501).



Il est nécessaire de procéder à des analyses d'impact ciblées pour évaluer les motifs qui justifient le recours à un système de reconnaissance de l'iris et la possibilité d'utiliser d'autres méthodes moins intrusives.

Ce système fonctionne parallèlement à un système de contrôle d'accès préexistant équipé d'un lecteur de badge sans contact.

Bien qu'il ne s'applique directement qu'à la BCE, l'avis du CEPD a servi plus généralement d'orientation sur les caractéristiques que doit revêtir un système biométrique respectueux de la vie privée. Le CEPD a notamment recommandé que la BCE procède à une analyse d'impact pour réexaminer la décision relative aux choix technologiques qu'elle a opérés. En effet, compte tenu de la nature extrêmement sensible des données biométriques, il est essentiel, avant de mettre en place une technique de ce type, de procéder à une analyse d'impact ciblée qui examine les raisons ayant justifié le recours à un système biométrique.

Le CEPD a également engagé la BCE à envisager la mise en œuvre, en temps voulu, d'un mode de recherche « un à un » où les données biométriques seraient stockées dans des puces plutôt que dans une base de données centrale. Par ailleurs, comme les systèmes biométriques ne sont pas accessibles à tous et qu'ils ne sont pas complètement exacts, il convient d'appliquer des procédures de secours facilement accessibles. Ces procédures respecteraient la dignité des personnes qui ne pourraient pas être engagées ou qui auraient pu faire l'objet d'une erreur d'identification, ce qui éviterait de leur faire porter le poids des imperfections du système.

Outre ce qui précède, le CEPD a recommandé que la BCE adopte un instrument législatif fournissant la base juridique des opérations de traitement visant à mettre en place un système de contrôle d'accès fondé sur l'utilisation de la biométrie.

### Recrutement

Le recrutement du personnel est, pour des raisons évidentes, une opération de traitement commune à tous les organes et institutions. Le CEPD a reçu un grand nombre de notifications dans ce domaine en 2008.

Le CEPD a procédé à un grand nombre de contrôles préalables des procédures de recrutement en vigueur dans les centres communs de recherche (CCR) de la Commission européenne. Ces procédures concernaient :

- les boursiers (dossier 2008-138) ;
- le personnel intérimaire (dossier 2008-139) ;
- les fonctionnaires (dossier 2008-140) ;
- les agents contractuels (dossier 2008-142) ;
- les stagiaires (dossier 2008-136).

Dans ces avis, le CEPD a mis en évidence la question de la collecte de certificats de bonne vie et mœurs dans le cadre de la procédure de recrutement et a demandé que la Commission européenne analyse au cas par cas le contenu du casier judiciaire ou du certificat de bonne vie et mœurs, de façon à ne collecter que les données pertinentes au regard des dispositions du Statut du personnel. Le CEPD a également encouragé le responsable du traitement à mettre en place un système permettant de supprimer les informations relatives à des infractions prescrites.

Le CEPD a reçu des notifications sur les procédures de recrutement au Parlement européen suivantes :

- recrutement des fonctionnaires et transfert interinstitutionnel (dossier 2004-207) ;
- agents temporaires (dossier 2007-323) ;
- agents contractuels (dossier 2007-384).

Des recommandations analogues ont été formulées en ce qui concerne la conservation des extraits de casier judiciaire. Le CEPD a également recommandé que la mention d'une éventuelle condamnation antérieure du candidat soit retirée des formulaires de candidature.

Le médiateur européen a également notifié la procédure de recrutement des fonctionnaires, agents temporaires et agents contractuels (dossier 2007-405).

De même, le Conseil a adressé une notification concernant la procédure de recrutement des fonctionnaires et autres agents (dossier 2007-194). Il a également été formulé une recommandation sur la conservation du casier judiciaire au terme de la procédure de recrutement.

Comme indiqué au point 2.3.2, le CEPD a lancé une nouvelle procédure de notification *a posteriori* concernant les opérations de traitement des données lors du recrutement dans les agences. Cela a conduit à l'élaboration d'orientations sur le traitement des données à caractère personnel dans les procédures de recrutement et donnera lieu à de nombreuses notifications dans ce domaine. Quelques agences ont déjà transmis des notifications dans le domaine du recrutement, notamment l'EMEA (dossier 2007-422), l'OHMI (Sélection de gestionnaires – dossier 2008-435), l'AESM (recrutement de personnel permanent, d'agents temporaires et d'agents contractuels – dossier 2007-566, et recrutement de stagiaires – dossier 2008-384) et l'OEDT (dossier 2008-157).

### Base de données des experts

Le CEPD a reçu une notification concernant la base de données des experts de l'EFSA (dossier 2008-455). Cette base de données contient des données professionnelles sur les experts scientifiques susceptibles d'être invités à exercer des fonctions consultatives pour l'EFSA (et pour les autorités nationales des États membres disposant d'un mandat analogue à celui de l'EFSA). Les candidats introduisent en ligne leur demande d'inscription dans la base de données. L'EFSA examine ensuite les candidatures pour que seuls les candidats répondant aux critères requis soient inscrits dans la base de données.

Le CEPD a notamment recommandé que l'attention de l'utilisateur final soit spécialement attirée sur les limites du contrôle de validité effectué par l'EFSA, suggérant qu'il utilise la base de données comme une réserve de candidatures et non comme une réserve d'experts dont les compétences et la fiabilité ont été soigneusement vérifiées individuellement par l'EFSA. Le CEPD a également recommandé que soient envoyés aux experts qui n'ont pas mis à jour leur profil (ou qui n'ont pas confirmé leur ancien profil) des rappels automatiques accompagnés d'un message d'avertissement indiquant que l'absence de réponse (après un certain nombre de rappels) entraînerait la suppression automatique de leur profil.

### Évaluation du personnel

Dans le domaine de l'évaluation du personnel, le CEPD a rendu un avis sur la notification en vue d'un contrôle préalable émanant du délégué à la protection des données du Parlement européen à propos de la base de données SKILLS (dossier 2008-192).

Cette base de données contient des données relatives à la carrière du personnel, portant sur l'expérience professionnelle au Parlement européen ainsi que sur l'expérience acquise avant l'entrée en fonctions au Parlement européen. Cette base de données constitue un traitement électronique qui facilite la gestion des ressources humaines pour tout ce qui a trait à la mobilité, à l'orientation professionnelle, à la recherche de personnel spécialisé, au pourvoi des postes vacants et à la planification de concours. Cette opération de traitement a pour base juridique l'article 197, paragraphe 2, du règlement intérieur du Parlement européen, qui prévoit le pouvoir d'organisation des services de l'institution. Étant donné le caractère général de cette base juridique, le CEPD a recommandé que, dans un souci de transparence et de sécurité juridique, l'autorité compétente au

sein du Parlement européen adopte une décision précisant les caractéristiques, la définition et les garanties de la base de données SKILLS.

Un autre avis sur une notification en vue d'un contrôle préalable relatif à l'évaluation du personnel concerne le système de contrôle interne de la qualité dans le cadre duquel les travaux des contrôleurs de marques de l'OHMI sont examinés et les résultats de cet examen sont enregistrés dans une base de données constituée à cette fin (dossier 2008-437). Ces contrôles ont pour objectif principal d'améliorer la qualité globale des résultats de l'OHMI. Toutefois, les résultats des contrôles sont également utilisés pour évaluer la qualité du travail de chaque évaluateur et informer la direction des décisions relatives aux mesures susceptibles d'avoir une incidence sur l'évaluateur, comme l'évaluation des performances, les promotions, le renouvellement de contrat, les mesures disciplinaires ou la formation.

Dans son avis, le CEPD a recommandé l'adoption d'une décision interne claire et formelle afin de renforcer le cadre juridique de l'opération et de garantir au personnel plus de clarté et de sécurité juridique. Cette décision devrait décrire clairement le système de contrôles de qualité *ex ante*, y compris leur finalité, et prévoir des garanties appropriées en matière de protection des données.

Le CEPD a également souligné que tous les efforts possibles devraient être mis en œuvre pour améliorer le niveau d'exactitude, de fiabilité et de cohérence des données. En tout état de cause, les données figurant dans la base de données ne devraient être que l'un des facteurs à prendre en considération dans le processus décisionnel. Chaque fois que des données figurant dans la base de données sont utilisées à des fins susceptibles d'avoir une incidence sur un membre du personnel, celui-ci doit également être entendu et avoir la possibilité de faire valoir son point de vue.

### Enquêtes de sécurité

Le CEPD a rendu un avis concernant les enquêtes de sécurité à la Commission européenne (dossier 2007-736). La direction « réquisitions administratives / sécurité » est habilitée à prendre certaines mesures contre les faits criminels ou délictueux visant les bâtiments occupés par la Commission, les personnes qui y travaillent ou qui y ont accès, ainsi que tous autres actes susceptibles de porter atteinte à cette institution. Cela inclut la conservation de tout élément de preuve, les recherches effectuées pour rassembler ces éléments, l'audition des déclarations

des plaignants, des témoins ou, le cas échéant, des auteurs des faits.

Le CEPD a examiné le traitement des données dans le cadre de la procédure des enquêtes de sécurité et a demandé que le service examine la proportionnalité des activités menées. Dans ce domaine, les enquêtes doivent être proportionnées non seulement à la finalité générale du traitement mais aussi à la finalité de chaque opération de traitement. Le CEPD a également souligné la nécessité d'offrir les garanties nécessaires à la protection des données et il a recommandé l'adoption d'un protocole spécifique à respecter dans le cadre des recherches de police scientifique. En ce qui concerne le transfert de données vers des pays tiers et des organisations internationales, le CEPD a recommandé que, dans les cas où le transfert est justifié uniquement sur la base de l'article 9, paragraphe 7, soit mis en place un registre contenant notamment des informations sur la finalité du transfert, les personnes concernées, le droit d'accès, la base juridique et la légalité du transfert, les destinataires des données ainsi qu'une indication de la période de conservation des données par le destinataire.

Le CEPD a également souligné le fait que le droit d'accès aux données à caractère personnel doit être établi comme principe et que toute exception à ce droit doit donc être appliquée de façon restrictive. Le CEPD a accepté sur cette base que l'article 20, paragraphe 1, point c), du règlement puisse servir à protéger les intérêts des dénonciateurs.

### **Procédure contre le harcèlement**

Le CEPD a rendu un avis sur la procédure informelle de lutte contre le harcèlement moral et le harcèlement sexuel à la Commission européenne (dossier 2008-062).

Le CEPD a notamment souligné le fait que le droit d'accès et de rectification, établi par les articles 13 et 14 du règlement, devrait aussi s'appliquer aux notes personnelles de la personne de confiance. Le CEPD a également recommandé que le droit d'accès au dossier concernant un harcèlement présumé s'applique également aux dossiers de tierces personnes si ces dossiers contiennent des données à caractère personnel concernant l'intéressé. Cela peut être le cas des personnes considérées comme « harceleurs » présumés ou comme témoins. Les informations figurant dans ces dossiers peuvent être obtenues directement par la personne concernée ou indirectement (notamment par l'intermédiaire du CEPD). Les limitations à ce droit d'accès peuvent

s'appliquer sur la base de l'article 20 du règlement, notamment pour protéger le droit d'accès d'autres personnes ou si cet accès risque de nuire à l'enquête en cours.

### **Coordination des dossiers par l'OLAF**

Le CEPD a rendu un avis concernant le traitement des données à caractère personnel par l'OLAF lors de l'ouverture d'un dossier de coordination (dossier 2007-699). Il s'agit de dossiers qui pourraient faire l'objet d'enquêtes externes de l'OLAF mais dans lesquels le rôle de l'OLAF est de contribuer aux enquêtes effectuées par d'autres services, nationaux ou communautaires, entre autres en facilitant la collecte et l'échange d'informations et en assurant une synergie opérationnelle entre les services nationaux et communautaires compétents. La plus grande partie du travail d'investigation est fournie par d'autres autorités. Le rôle de l'OLAF consiste notamment à faciliter les contacts et à encourager les autorités compétentes à coopérer. Les catégories de données à caractère personnel traitées par l'OLAF dans ces dossiers concernent les données d'identification, les données professionnelles et les informations concernant les activités liées aux éléments qui font l'objet de la coordination.

Dans son avis, le CEPD a demandé à l'OLAF de veiller à ce que les personnes concernées soient informées du traitement de données qui a lieu dans le cadre de la coordination. Cela pourrait prendre la forme d'informations fournies par les autorités nationales compétentes, comprenant dans la déclaration de confidentialité adressée aux personnes concernées un paragraphe les informant de la possibilité d'un transfert à l'OLAF, à des fins de coordination, des données à caractère personnel les concernant. Puisque les intéressés auront été informés du transfert à l'OLAF des données à caractère personnel les concernant, il ne sera plus nécessaire que l'OLAF fournisse de nouveau cette information. Le CEPD a également suggéré dans son avis d'apporter quelques modifications à la déclaration de confidentialité et demandé à l'OLAF de procéder à une première évaluation de la nécessité de prévoir une période de vingt ans au regard de la finalité d'un tel délai de conservation.

### **Autorisation de témoigner en justice**

Le CEPD a procédé au contrôle préalable de la procédure mise en place par la Commission européenne en vue de respecter les dispositions du statut du personnel relatives à l'autorisation de témoigner en justice. Selon l'article 19 du statut,

« le fonctionnaire ne peut faire état en justice, à quelque titre que ce soit, des constatations qu'il a faites en raison de ses fonctions, sans l'autorisation de l'autorité investie du pouvoir de nomination. Cette autorisation ne peut être refusée que si les intérêts des Communautés l'exigent et si ce refus n'est pas susceptible d'entraîner des conséquences pénales pour le fonctionnaire intéressé. Le fonctionnaire reste soumis à cette obligation même après la cessation de ses fonctions. »

Dans son avis, le CEPD a formulé des recommandations relatives au droit de la défense, à savoir que le fonctionnaire doit avoir la possibilité de s'exprimer avant la décision de l'autorité investie du pouvoir de nomination à condition qu'il n'existe aucune limitation découlant de l'article 20, paragraphe 1, du règlement (CE) n° 45/2001.

### 2.3.5. Principales questions soulevées par les cas de contrôle préalable

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. C'est l'objet de l'article 27 du règlement (CE) n° 45/2001. Parallèlement aux dossiers de contrôle préalable *a posteriori*, dix-huit dossiers de contrôle préalable proprement dit<sup>(8)</sup> ont été notifiés au CEPD en 2008. Ces dossiers ont donné lieu à seize avis du CEPD (voir le point 2.3.3).

#### Procédures de sélection

Le CEPD a reçu de l'Agence des droits fondamentaux de l'Union européenne (FRA) une notification en vue d'un contrôle préalable relatif au traitement des données à caractère personnel, dans le cadre de la procédure de sélection des membres du comité scientifique de l'Agence. Il a reçu par la suite une notification du Parlement européen concernant le traitement des données à caractère personnel par la commission LIBE (commission des libertés civiles, de la justice et des affaires intérieures) dans le cadre de l'étape suivante de cette procédure de sélection.

Ces deux notifications concernant la même procédure de sélection, le CEPD a rendu un seul avis concernant l'intégralité de la procédure de sélection (dossiers 2008-179 et 2008-202).

<sup>(8)</sup> C'est-à-dire portant sur des traitements dont la mise en œuvre n'a pas encore débuté.

De son analyse, le CEPD a avant tout dégagé des recommandations dans le domaine de l'information communiquée à la personne concernée. De fait, bien que la procédure ait déjà été lancée, les candidats n'ont pas été informés que les renseignements qu'ils avaient transmis dans le cadre de la procédure de sélection (CV, lettre de motivation, etc.) seraient rendus publics du fait de la nature publique des réunions de la commission LIBE. Conformément à l'article 12 du règlement, ces informations devraient être fournies au moment de la collecte des données ou au plus tard au moment où les données sont communiquées pour la première fois à un tiers. Comme cette information n'apparaît pas dans l'appel à manifestation d'intérêt, le CEPD a recommandé que :

- la FRA informe tous les candidats présélectionnés que les données qu'ils ont fournies vont être mises à la disposition du public à cause de la nature publique des sessions du Parlement européen, et ce avant la transmission de leurs données à la commission LIBE. Il a également recommandé que la FRA les informe de leur droit de s'opposer à la publication des données les concernant ;
- la FRA informe les candidats présélectionnés des procédures à suivre pour exercer leur droit d'accès et de leur droit de saisir le CEPD.

Le CEPD a également recommandé que ces informations figurent sur le site Internet de la FRA afin qu'elles soient aussi accessibles aux candidats qui n'ont pas été présélectionnés. Le CEPD estime que les informations concernant le traitement des données à caractère personnel devraient être disponibles sur le site Internet de la FRA, au moins jusqu'à la fin de la procédure de sélection.

Le CEPD a également procédé au contrôle préalable<sup>(9)</sup> du traitement des données à caractère personnel dans le cadre de la procédure de sélection du CEPD et du délégué à la protection des données (DPD). Deux avis ont été rendus dans ce domaine, le premier concernant la procédure de la Commission européenne relative à la constitution d'une liste de candidats présélectionnés à soumettre au Conseil et au Parlement européen (dossier 2008-222) et le second sur la procédure appliquée au Conseil et au Parlement (dossiers 2008-280 et 2008-292).

<sup>(9)</sup> Ce contrôle s'est déroulé sous la responsabilité du contrôleur adjoint, qui n'était pas concerné par la procédure de sélection.

En ce qui concerne la première partie de la procédure, le CEPD a déclaré qu'à tous les stades de la procédure, il est rappelé aux destinataires auxquels les données sont communiquées qu'ils ne peuvent traiter ces données qu'aux fins de la présélection de candidats aux postes de CEPD et de Contrôleur adjoint. Le CEPD a en outre noté que l'application CV-Online est utilisée et que cet outil demande l'indication du numéro personnel des personnes travaillant dans les institutions de l'UE. Étant donné que l'application CV-Online est un outil informatique standard utilisé pour toutes les procédures de sélection de hauts fonctionnaires à la Commission, tant en interne qu'en externe et que, dans certains cas, ce numéro pourrait s'avérer nécessaire lors de la phase de sélection de ces autres procédures, le CEPD a recommandé que la Commission mentionne clairement sur la page d'instructions communiquées aux candidats que l'indication du numéro personnel sur le formulaire de candidature à remplir sur CV-Online est entièrement facultative et que les candidats ne sont pas tenus de remplir ce champ. Il a particulièrement insisté sur l'importance d'informer les candidats de ce que leurs données seraient mises à la disposition du public, du fait de la nature publique des réunions de la commission LIBE.

En ce qui concerne la partie suivante de la procédure qui se déroule au Parlement européen et au Conseil, le CEPD a rendu un avis distinct dans lequel il souligne l'importance de fournir des informations appropriées sur le traitement des données à caractère personnel aux candidats présélectionnés dans les deux institutions.

### **Suivi individuel/projet pilote**

Une notification en vue d'un contrôle préalable a été transmise au CEPD au sujet d'un projet pilote concernant le suivi de la productivité individuelle au Conseil (dossier 2008-436). En vue de donner aux chefs des unités linguistiques et aux membres du personnel des indicateurs de performance individuels, l'outil proposé devrait permettre à chaque personne concernée de suivre sa propre production et au chef d'unité de la personne concernée de suivre la production de tout membre de son unité ainsi que de suivre, en une seule opération, la production de l'ensemble des membres de l'unité.

L'opération de traitement a été soumise au contrôle préalable, tout d'abord parce que les résultats du projet pilote seront utilisés par le chef d'unité de la personne concernée comme élément d'appréciation de la production de chaque membre du personnel, notamment lors de l'exercice de notation, et le traitement des données a donc pour objectif d'évaluer l'efficacité des membres du personnel (article 27, paragraphe 2, point b)). Ensuite, le traitement implique des interconnexions entre deux bases de données qui ne sont pas prévues par la législation nationale ou communautaire (article 27, paragraphe 2, point c)).

Le CEPD a saisi l'occasion de ce contrôle préalable pour rappeler au Conseil la politique à suivre en ce qui concerne les projets pilotes. En principe, le projet ne doit pas commencer avant la mise en œuvre des recommandations formulées par le CEPD dans son avis. Par ailleurs, l'achèvement d'un projet pilote ne déclenche pas automatiquement le déploiement complet du système, de sorte que ce dernier ne peut être mis en place immédiatement. En effet, il s'impose d'analyser les résultats générés par la phase pilote avant de généraliser l'application du système. Les résultats du projet pilote doivent être communiqués au CEPD avant que le projet général ne soit lancé et le CEPD doit être informé de toute modification du système général qui pourrait altérer le traitement des données à caractère personnel. Le CEPD analyse ensuite les résultats du projet pilote ainsi que toute implication sur la protection des données avant le lancement du système général. Dans sa recommandation, le CEPD souligne que si le projet pilote devait se transformer en un projet à part entière au terme du projet pilote, il conviendrait d'adopter une décision ou un instrument juridique offrant une base juridique spécifique au traitement des données à caractère personnel.

### **Horaire flexible**

Le CEPD a rendu un autre avis fondé sur l'article 27, paragraphe 2, point c), du règlement (CE) n° 45/2001 à propos du dossier « Interface Flexitime – Persona Grata » du Conseil (dossier 2008 324). PersonaGrata est un outil de gestion du personnel qui sert à organiser le travail dans les services de traduction du Conseil. La finalité de l'interface est

d'importer les données de la base Flexitime vers PersonaGrata de façon à éviter le double encodage de données considérées comme équivalentes entre les deux bases.

Le CEPD a estimé que l'enregistrement des données n'est pas équivalent car cette catégorie de données est spécifique d'un système Flexitime. En outre, le nombre de saisies liées aux absences dans le système Flexitime est supérieur à celui de PersonaGrata. Les différents motifs d'absence ont donc été présentés aux utilisateurs comme un seul et unique motif d'absence dans le système PersonaGrata. Le CEPD a souligné que l'équivalence des données dans les deux systèmes pourrait contribuer à garantir le respect du principe de la qualité des données.

Le CEPD a également rendu un avis sur le traitement des données dans le cadre de l'horaire mobile spécifique de la DG Entreprise et Industrie de la Commission européenne <sup>(10)</sup> (dossier 2008-111). Dans cette opération de traitement, la DG Entreprise et Industrie prévoyait d'installer une interface sur les ordinateurs personnels (PC) afin de collecter les données relatives à la présence du personnel.

Dans son analyse, le CEPD a estimé que la finalité du traitement notifié par la DG Entreprise et Industrie ne correspond pas tout à fait à celle de Flexitime, telle qu'elle ressort de l'examen du système de gestion du temps (TIM) de la Commission européenne. De fait, dans le dossier notifié, si les données devaient être conservées temporairement par le chef d'unité, cela pourrait mener à une évaluation non prévue par le système TIM. Le CEPD est donc opposé à l'envoi de courriers électroniques vers la boîte fonctionnelle des chefs d'unité. Ceci dit, le CEPD a admis que l'idée de pouvoir disposer d'une interface conviviale pour enregistrer les pointages dans TIM sans devoir recourir à l'interface utilisateur graphique de SYSPER2-TIM mérite d'être mise en œuvre.

### Contrôle des communications électroniques

Le contrôle de l'utilisation de l'Internet par le personnel d'une institution ou d'un organe de l'UE

<sup>(10)</sup> Le système de gestion du temps (TIM) intégrant l'horaire mobile dans l'outil de gestion du personnel (Sysper 2) de la Commission européenne a déjà fait l'objet d'un contrôle préalable (dossier 2007-063).



Un contrôle dissimulé de l'utilisation d'Internet, dont les utilisateurs ignorent l'existence, n'est pas acceptable.

a donné au CEPD l'occasion de marquer sa préférence pour une approche préventive plutôt que répressive de l'utilisation abusive d'Internet, et de rappeler la nécessité du principe de proportionnalité quant aux moyens employés (dossier 2008-284).

À cet égard, le CEPD a notamment conclu que, en l'absence de suspicion fondée, le contrôle de tous les URL visités par tous les utilisateurs est inutile et excessif. Afin de détecter les abus, le CEPD a conseillé d'utiliser des indicateurs (volume de données téléchargées, temps passé sur l'Internet, nombre élevé d'échecs de connexion à des sites bloqués, etc.) sans passer par un contrôle des URL. Le CEPD a néanmoins admis que dans certaines circonstances, il peut s'avérer nécessaire de contrôler les URL consultés par certaines personnes. Tel est le cas s'il existe une suspicion fondée qu'un utilisateur adopte un comportement contraire à l'institution (par exemple, le téléchargement d'images pédophiles) ou si la longueur des URL peut être un indice de tentative d'attaque par URL.

### Système de télévision en circuit fermé

Le CEPD a rendu un avis sur le système de télévision en circuit fermé (CCTV) que l'Office européen de lutte antifraude (OLAF) exploite dans ses locaux de Bruxelles à des fins de sécurité (dossier 2007-634). Cet avis est le premier des avis du CEPD concernant la vidéosurveillance. Pour de plus amples informations sur ce dossier, prière de se reporter au point 2.7.2.

### Contrôle d'accès et d'identité

Le CEPD a rendu un avis concernant le système de contrôle d'accès et d'identité de l'OLAF (dossier 2007-635). Ce système fait partie de l'infrastructure de sécurité qui protège les locaux de l'OLAF et ses systèmes informatiques. Ce système est destiné à contrôler l'identité des personnes entrant et sortant des locaux de l'OLAF en dehors des heures de service, ainsi que des zones spéciales sécurisées, et à leur en autoriser ou refuser l'accès. Pour ce faire, l'OLAF utilise des cartes à puce et un système d'authentification par les empreintes digitales. Les données biométriques relatives aux utilisateurs sont uniquement stockées sur la carte à puce et ne peuvent être utilisées à d'autres fins.

S'agissant du contrôle d'accès de l'OLAF, le CEPD a interprété le principe du besoin d'en connaître comme exigeant que seules les personnes qui ont besoin d'un accès spécial soient enregistrées dans le système et, par conséquent, fassent l'objet d'un relevé d'empreintes. Ainsi, le CEPD a recommandé que l'OLAF réexamine la question et envisage la possibilité de limiter la liste des personnes dont les empreintes devront être enregistrées, au vu des besoins réels en termes d'accès à l'OLAF en dehors des heures normales de service, ou d'accès aux zones sécurisées au sein de l'OLAF, ou encore d'utilisation des points d'accès non surveillés (cages d'escalier) aux locaux sécurisés de l'OLAF.

L'OLAF prévoit de conserver les données enregistrées (ou les informations concernant le contrôle d'accès) pendant une durée maximale d'un an aux fins d'enquête sur les incidents touchant à la sécurité. Le CEPD a reconnu qu'il peut être nécessaire de conserver l'historique de l'enregistrement des données pendant une période qui permette de reconstituer les événements intervenus pendant les incidents de sécurité et que, dans le cas de l'OLAF, une période très courte pourrait créer des difficultés pratiques. Le CEPD a toutefois souligné que l'OLAF devrait mettre au point une procédure d'identification des incidents et de réaction à ceux-ci, afin qu'ils soient détectés et signalés dès que possible. Il a également invité l'OLAF à réexaminer la période qu'il a fixée en réexaminant la nécessité d'en raccourcir la durée sur la base de statistiques relatives aux incidents.

Le CEPD a également rendu un avis concernant le traitement des données à caractère personnel effectué par l'OLAF afin de s'assurer que seules les personnes autorisées ont accès aux systèmes informatiques de l'OLAF et de pouvoir mener des

enquêtes sur les incidents de sécurité (« Core Business Information System » – CBIS) (dossier 2008-223). L'authentification dans le CBIS repose sur des certificats et des empreintes digitales numériques. Les certificats sont stockés sur les badges personnels (cartes à puce) des utilisateurs et protégés par un programme d'authentification biométrique « match-on-card » (concordance entre les empreintes de l'utilisateur et les données contenues dans la carte). Chaque utilisateur aura trois modèles d'empreintes digitales stockées sur son badge OLAF, qui est une interface de contact utilisée par le système d'authentification informatique CBIS.

Dans son avis, le CEPD a analysé en particulier le respect du principe de la qualité des données. À cette fin, il a analysé de manière approfondie la mise en œuvre des procédures de secours en cas d'enregistrement impossible. Bien que le CEPD ait estimé que la solution proposée par l'OLAF diminue le risque d'enregistrement impossible, ce risque existe et dans un tel cas, la situation serait discriminatoire. C'est pourquoi le CEPD suggère que l'OLAF mette en œuvre une solution de remplacement réaliste pour les cas d'enregistrement impossible permanent. Il a en outre examiné la définition du taux de faux rejets et recommandé que l'OLAF fixe un taux de faux rejet précis, qui reflète la politique qu'il a adoptée en matière de sécurité.

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

Au cours de l'année 2008, le nombre de consultations quant à la nécessité d'un contrôle préalable par le CEPD est resté stable : vingt consultations en 2008 comme en 2007.

Plusieurs dossiers ont été déclarés soumis au contrôle préalable :

- recrutement de personnel intérimaire ;
- publication des points de promotion ;
- infractions aux règles de la circulation ;
- données biométriques et contrôle de l'accès.

Certains traitements 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 les infractions aux règles de la circulation routière au Conseil 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 traitement des données biométriques et des données relatives au contrôle de l'accès a été considéré comme devant faire l'objet d'un contrôle préalable en cas d'utilisation d'un système de correspondance biométrique. En effet, ces systèmes présentent des risques particuliers au regard des droits et libertés des personnes concernées. Le CEPD fonde son point de vue principalement sur la nature des données biométriques, qui sont extrêmement sensibles en raison de certaines des caractéristiques propres à ce type de données. Ainsi, les données biométriques modifient irrévocablement la relation entre le corps et l'identité en ce sens qu'elles rendent les caractéristiques du corps humain « lisibles par une machine » et susceptibles d'être utilisées ultérieurement. Outre la nature extrêmement sensible de ces données, le CEPD note également les possibilités d'interconnexions et la situation actuelle en termes d'outils technologiques, qui peuvent avoir des conséquences inattendues et/ou fâcheuses pour les personnes concernées.

Le CEPD a conclu que le traitement des données relatives aux enquêtes du délégué à la protection des données 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 ni à évaluer leur responsabilité. Par ailleurs, l'évaluation par le délégué à la protection des données d'une violation des dispositions du règlement (CE) n° 45/2001 recouvre une notion plus large que celle de suspicion, d'infraction ou de condamnation pénale. Le fait que des données relatives à des suspicions, infractions ou condamnations pénales puissent éventuellement apparaître ne modifie pas le champ d'application du traitement.

Le dossier relatif à l'accès aux documents confidentiels n'a pas été soumis au contrôle préalable car la nature du champ d'application du traitement ne relève pas du champ d'application de l'article 27 du règlement. En effet, si des données relatives à la santé, à des suspicions, infractions, condamnations pénales ou mesures de sûreté figurent dans les documents confidentiels, la finalité du traitement n'est pas de traiter ces données mais seulement d'enregistrer les personnes qui ont accès à ces documents.

### 2.3.7. Notifications non soumises au contrôle préalable ou retirées

En 2008, le CEPD a également examiné douze dossiers pour lesquels il a conclu qu'ils n'étaient

pas soumis au contrôle préalable (soit 9,91 % des dossiers qui lui ont été soumis). Il est parvenu à ces conclusions à l'issue d'un examen approfondi des notifications. Néanmoins, ces examens ont donné lieu à des recommandations du CEPD. Deux de ces dossiers concernaient le domaine des télécommunications, deux le contrôle de l'accès, sept <sup>(11)</sup> le domaine du personnel et un d'autres domaines tels que « Advanced Records System (ARES) » et la *Nomenclature commune* (Nomcom).

Parmi les sept dossiers concernant la question du personnel, un dossier portait sur la gestion du temps de travail <sup>(12)</sup>. Le CEPD a conclu que ce traitement ne doit pas être soumis à un contrôle préalable car cette notification est à mettre en relation avec la notification concernant le système général Flexitime <sup>(13)</sup> et le traitement n'a pas fait l'objet de changement substantiel. Le CEPD a néanmoins formulé des recommandations sur la période de conservation des données.

En ce qui concerne le contrôle de l'accès, l'une de ces notifications <sup>(14)</sup> a été soumise au titre de l'article 27, paragraphe 2, point a), du règlement (traitement de données relatives aux mesures de sûreté présentant un risque particulier). Selon l'interprétation du CEPD, les « mesures de sûreté » visées à l'article 27, paragraphe 2, point a), ne portent pas sur la protection physique des bâtiments et du personnel mais désignent plutôt les mesures prises à l'égard des personnes physiques dans le cadre de procédures pénales (ou administratives).

Le CEPD a également examiné si d'autres aspects du traitement nécessitaient un contrôle préalable. L'utilisation de la technologie RFID est un aspect important à cet égard. Le CEPD considère que la RFID en elle-même, sans autre élément additionnel, ne présente pas de risques particuliers au sens de l'article 27, paragraphe 1. Cela ne signifie

<sup>(11)</sup> « Entités légales » et identification bancaire à l'OEDT (dossier 2008-168), traitement relatif au paiement des salaires à FRA (dossier 2008-396), procédure d'évaluation à l'OHMI (dossier 2008-415 mise à jour de la notification), gestion du personnel de la Commission au CCR-ITU à Karlsruhe (dossier 2008-151, bien que les utilisations de la base de données soient liées à des traitements bien distincts, elles n'ont pas été décrites avec suffisamment de détail dans la notification), Commission – CCR Karlsruhe – horaire mobile ZEUS (dossier 2008 486), dossiers personnels du Cedefop (dossier 2008-197) et le traitement Superviseo du Médiateur (dossier 2008 052, outil non destiné à l'évaluation).

<sup>(12)</sup> Commission – CCR Karlsruhe – ZEUS Flexitime (dossier 2008-486).

<sup>(13)</sup> Commission – « Sysper 2 : module Time management » (TIM) (dossier 2007-063).

<sup>(14)</sup> Cedefop (dossier 2008-195).

toutefois pas qu'il n'est pas nécessaire de recommander d'utiliser les meilleures pratiques afin de garantir le respect de la vie privée et la protection des données. Des recommandations ont néanmoins été formulées au sujet de la finalité exacte du traitement, de la description du contrôle interne de l'accès, de l'information de la personne concernée, de la période de conservation des données et des mesures techniques de sécurité.

Parmi les dix dossiers retirés, il convient de mettre en évidence un dossier particulier de la Banque européenne d'investissement (BEI) concernant les « personnes politiquement exposées » (dossier 2007-543). Le CEPD a reçu une notification en vue d'un contrôle préalable relatif à une procédure concernant les personnes politiquement exposées que la BEI a mis en place en vue de se conformer aux dispositions de la directive 60/2005/CE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme. Cette notification a ensuite été retirée car le manuel « Base de données des personnes politiquement exposées » initialement prévu avait peu de chance d'être établi dans l'avenir. D'autres outils de contrôle sont à l'étude ; ils seront soumis en temps voulu au CEPD pour contrôle préalable.

Dans l'attente de l'adoption d'autres outils de contrôle, les contrôles effectués par le chef du Bureau de conformité sont menés en vue d'assurer la conformité avec la directive 60/2005/CE. Le CEPD a donc formulé des recommandations, notamment en ce qui concerne les périodes de conservation des données et les informations à communiquer à la personne concernée.

En ce qui concerne la période de conservation des données, la BEI a fixé une durée de quinze ans afin de prendre en compte, outre les dates limites générales des actions civiles, les éventuelles demandes d'accès ayant un lien avec le terrorisme ou d'autres délits, présentées par les autorités d'autres pays du monde. Le CEPD a invité la BEI à réexaminer la période de conservation des données, fixée à 15 ans, en fonction des demandes d'information effectives présentées par les autorités nationales.

En ce qui concerne l'obligation d'informer la personne concernée, conformément aux articles 11 et 12 du règlement, le CEPD a reconnu qu'informer chaque personne politiquement exposée risquait dans certains cas d'interrompre et d'annuler l'efficacité des activités que mène la BEI en vertu de la directive en matière de prévention du blanchiment

de capitaux. À cet effet, les dérogations à l'obligation d'informer, prévues à l'article 20, paragraphe 1, points a), b) et c), du règlement, peuvent s'appliquer. Par ailleurs, étant donné que dans de nombreux cas, la BEI n'a pas de relations contractuelles directes avec les personnes concernées, la dérogation prévue à l'article 12, paragraphe 2, peut aussi être appliquée. Le CEPD était prêt à accepter, comme solution de remplacement de l'information individuelle, la publication, sur le site web de la BEI et dans sa documentation, d'une note d'information générale concernant les procédures de traitement des données relatives aux personnes politiquement exposées.

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

Lorsque le CEPD rend un avis relatif à 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.

En outre, le CEPD peut 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), ou adresser un avertissement ou une admonestation au responsable du traitement. Il peut aussi ordonner la rectification, le verrouillage, l'effacement ou la destruction de toutes les données, ou interdire temporairement ou définitivement un traitement. Dans le cas où les décisions du CEPD ne seraient pas respectées, celui-ci a le droit de saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité CE.

Tous les cas de contrôle préalable ont abouti à des recommandations. Comme expliqué plus haut (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. Le CEPD a demandé, dans la lettre formelle transmise avec son avis, que l'institution ou l'organe concerné l'informe, dans un délai de trois mois, des mesures adoptées pour mettre en œuvre les recommandations. En 2008, le CEPD a clos trente-six dossiers, soit à peu près le même nombre qu'en 2007. Ce chiffre devrait augmenter en 2009 car le processus de suivi a été lancé ou réaffirmé pour un grand nombre de dossiers.

### 2.3.9. Conclusions et perspectives

Comme les années précédentes, les contrôles préalables, et notamment les contrôles préalables effectués *a posteriori*, ont constitué un outil très important pour la supervision des institutions et organes communautaires.

Les conclusions pour 2008 peuvent être résumées comme suit :

- 2008 a été une année de travail intense, avec 105 avis rendus, soit un nombre supérieur à celui de 2007 (90 avis).
- Ce résultat a été obtenu en diminuant le nombre de jours nécessaires à l'élaboration des avis et en réduisant nettement le nombre de jours de prolongation nécessaires.
- En revanche, le nombre de jours de suspension nécessaires pour la réception des informations adressées par les responsables du traitement ou les délégués à la protection des données a augmenté de façon alarmante.
- Afin de faciliter à la fois les notifications et l'élaboration des avis, le contrôle préalable *a posteriori* des opérations de traitement dans les agences fait l'objet d'une nouvelle procédure selon une approche thématique systématique.
- Certaines questions importantes ont été examinées pour la première fois, notamment le service de gestion de l'identité, le contrôle d'accès au moyen d'un système de reconnaissance de l'iris ou d'une authentification par les empreintes digitales, les enquêtes de sécurité, le contrôle de l'utilisation d'internet par le personnel, le système de télévision en circuit fermé, etc.

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

- Les principales institutions devraient compléter leurs notifications dans tous les domaines relevant de l'article 27 du règlement et les agences devraient accomplir des progrès sensibles en vue de se conformer à cette obligation.
- Le temps nécessaire pour répondre aux demandes de complément d'information formulées par le CEPD doit être fortement réduit, notamment grâce à l'élaboration satisfaisante des notifications et des annexes.
- Certains domaines, tels que celui de la vidéosurveillance, vont connaître des progrès importants, grâce à l'application de la nouvelle politique consistant à limiter les contrôles préalables aux systèmes qui s'écartent des pratiques « courantes » prévues dans les lignes directrices (voir le point 2.7).
- Le suivi des recommandations se poursuivra grâce aux informations communiquées par les responsables des traitements (voir le point 2.3.8) et aux vérifications (voir le point 2.5).

## 2.4. Plaintes

### 2.4.1. Introduction

L'article 41, paragraphe 2, du règlement (CE) n° 45/2001 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>

<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 ».

Conformément aux articles 32 et 33 du règlement <sup>(16)</sup>, toute personne physique peut présenter une réclamation au CEPD indépendamment de sa nationalité ou de son lieu de résidence. Les membres du personnel des institutions et organismes de l'UE visés au statut peuvent également soumettre une réclamation 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 réclamation, il envoie un accusé de réception à l'auteur de la réclamation, sans se prononcer sur sa recevabilité, sauf dans le cas où la réclamation est manifestement irrecevable, sans qu'il soit nécessaire de procéder à un examen complémentaire. Le CEPD demande aussi à l'auteur de la réclamation de l'informer d'éventuelles autres actions (pendantes ou non) engagées devant une juridiction nationale, la Cour de justice des Communautés européennes ou auprès du médiateur européen.

Si la réclamation est recevable, le CEPD procède à une enquête, s'il y a lieu, notamment en contactant l'institution ou l'organe concerné ou en demandant des renseignements complémentaires à l'auteur de la réclamation. Le CEPD est habilité à obtenir du responsable du traitement, de l'institution ou de l'organe concerné 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, une institution ou un organe exerce ses activités.

<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 réclamation au sens de l'article 90, paragraphes 1 et 2, dans le cadre de ses compétences.

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 ou l'organe, le CEPD met en place un suivi avec l'institution ou l'organe concerné.

En 2008, le CEPD a reçu quatre-vingt-onze plaintes, dont vingt-trois ont été déclarées recevables et ont fait l'objet d'un examen plus poussé par le CEPD. La plupart des autres 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.

En 2008, vingt et une plaintes recevables ont été traitées. Certaines d'entre elles sont brièvement présentées ci-après.

## 2.4.2. Plaintes déclarées recevables

### Collecte ou transfert de données excessives

Le CEPD a reçu une réclamation d'un membre du personnel de la Commission européenne concernant la demande adressée par cette dernière pour obtenir un certificat d'imposition belge complet du conjoint afin de vérifier les droits à la couverture complémentaire en soins de santé (dossier 2008-370). Après enquête, le CEPD a conclu que cette demande était excessive et qu'elle n'était pas conforme au principe du caractère adéquat des données prévu à l'article 4, paragraphe 1, points b) et c), du règlement. À la suite de l'enquête du CEPD, il a été mis fin à cette pratique et la Commission ne collecte les données figurant dans le certificat

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

d'imposition belge que dans la mesure où le revenu professionnel est concerné, toutes les autres sources de revenu pouvant être masquées.

Une autre réclamation a été adressée par un comité du personnel et différents membres du personnel de l'OHMI concernant le traitement de données à caractère personnel dans le cadre d'un système de contrôle de la qualité (dossier 2008 0119). Les auteurs de la réclamation ont demandé au CEPD d'étudier la question et de confirmer que :

- la connexion de deux bases de données possibles à des fins autres qu'historiques, statistiques ou scientifiques n'affecte pas les membres du personnel ;
- les données collectées sont adéquates et pertinentes ;
- les données sont effectivement non excessives, compte tenu des nombreuses statistiques sur la productivité des examinateurs qui sont déjà disponibles aux fins d'évaluation ;
- les données collectées sont exactes ;
- les données ne sont pas conservées pour une durée plus longue que nécessaire.

Le CEPD a estimé que la réclamation était recevable tant de la part du représentant du comité du personnel que des membres du personnel, en application des articles 33 et 90 du statut, et qu'il était compétent. Il a conclu qu'il n'y avait a priori pas de violation du principe de la qualité des données, ni des règles régissant leur conservation.

Cela étant, la procédure à l'examen visait à évaluer la qualité du travail effectué par les examinateurs et, en particulier, fait partie de l'exercice d'évaluation. Le CEPD a donc considéré que la procédure entrant en ligne de compte pour un contrôle préalable. Le contrôle préalable devrait normalement intervenir avant la mise en place d'une procédure, même si celle-ci est seulement en phase de test et n'est établie que pour quelques mois. Par voie de conséquence, l'instauration du nouveau système de contrôle de la qualité sans notification au CEPD en vue d'un contrôle préalable constituerait une violation du règlement (CE) n° 45/2001. Conformément aux compétences qui lui sont conférées en vertu de l'article 47, paragraphe 1, point b), du règlement, le CEPD a invité l'instance concernée à notifier le traitement de données à caractère personnel résultant du système de contrôle de la qualité en vue d'un contrôle préalable conformément à l'article 27, paragraphe 1.

Dans un autre dossier, l'auteur de la réclamation a affirmé que la Commission européenne avait transmis aux services de transport par autobus de la ville de Luxembourg les prénoms et noms de tous les membres du personnel travaillant dans les institutions européennes à Luxembourg (dossier 2008 421). Il s'agissait de délivrer une carte de transport gratuit par bus, sur laquelle n'apparaissaient ni le nom ni le prénom mais seulement un numéro. L'auteur de la réclamation estimait que cette façon de faire n'était ni nécessaire ni proportionnelle et qu'elle violait les principes de la protection des données.

Le CEPD a enquêté sur la question et il a relevé que la Commission avait transmis à son personnel, avant que le traitement n'ait eu lieu, une note d'information lui fournissant tous les éléments nécessaires conformément aux articles 11 et 12 du règlement (CE) n° 45/2001. Les personnes concernées se sont vu donner la possibilité d'accepter ou de refuser le transfert de leurs noms et prénoms aux services d'autobus de la ville de Luxembourg. Par conséquent, dans ce contexte, l'élément de consentement justifiait la licéité du transfert en question en vertu de l'article 5, point d), du règlement. En outre, le CEPD a estimé que l'initiative de la Commission visant à délivrer des cartes de transport gratuit par autobus constituait une mission effectuée dans l'intérêt public, sachant que le statut prévoit que les institutions puissent adopter des mesures de nature sociale pour le bien-être de leur personnel. Cet élément supplémentaire pourrait donc justifier la licéité du transfert en vertu de l'article 5, point a), du règlement.

#### Accès aux données

Un membre du personnel du Parlement européen a adressé une réclamation au CEPD en alléguant que l'unité du Parlement chargée de la gestion des congés de maladie lui avait refusé d'exercer son droit d'accès à son dossier médical et son droit de rectification de celui-ci (dossier 2007 681).

Dans son analyse juridique, le CEPD a notamment donné une interprétation non restrictive de l'article 13 du règlement (CE) n° 45/2001 et a estimé que l'auteur de la réclamation avait non seulement le droit d'accéder à son dossier médical mais également le droit d'obtenir une copie ou une photocopie de ses propres données médicales sans limitation du nombre d'exemplaires. S'agissant du droit

de la personne en question à rectifier les données la concernant, le CEPD a indiqué que, même s'il est impossible de rectifier des évaluations médicales, l'auteur de la réclamation devrait avoir le droit de mettre à jour son dossier médical en y ajoutant d'autres avis médicaux. S'agissant de la demande adressée par l'auteur de la réclamation pour que son dossier médical soit transféré au médecin qu'il avait désigné, le CEPD a considéré que la nécessité d'un tel transfert était démontrée par le consentement explicite de la personne concernée, qui prouvait également que ce transfert n'aurait pas pu porter préjudice à ses intérêts légitimes.

La décision du CEPD relative à cette réclamation a revêtu un intérêt particulier pour le syndicat SFIE du Parlement européen, qui a transmis au personnel de l'institution un courrier électronique mentionnant les recommandations du CEPD.

Une autre réclamation a été reçue concernant une violation présumée de l'article 13 du règlement (CE) n° 45/2001 par la Commission européenne et l'Office européen de sélection du personnel (EPSO) suite au refus d'accès aux résultats d'examen obtenus dans le cadre d'un concours général organisé par l'EPSO (dossier 2007 0250). Le CEPD a considéré que, sur la base de l'article 13 du règlement, l'auteur de la réclamation avait le droit d'accéder aux résultats ou points qu'il avait obtenus durant les épreuves de présélection écrites et orales du concours général de l'EPSO. Ce droit pourrait faire l'objet de certaines limitations en vertu de l'article 20, paragraphe 1, point c), du règlement. Il se pourrait en particulier que les noms des autres candidats figurant dans les résultats des tests comparatifs de l'auteur de la réclamation doivent être enlevés ou masqués et que l'identification des membres du comité de sélection doive – si nécessaire – être rendue impossible. À la suite de l'intervention du CEPD, l'EPSO a accepté de communiquer à la personne concernée les résultats de test demandés et le dossier a été clôturé.

Un ancien fonctionnaire de la Commission européenne a introduit une réclamation intéressante concernant l'accès à des données à caractère personnel « inexistantes » (dossier 2008 0438). L'auteur de la réclamation s'est plaint de ce que la Commission avait mentionné dans une lettre qu'elle lui avait adressée une étude comparative contenant des données à caractère personnel le concernant. Invitée à communiquer l'étude, la Commission a refusé en faisant valoir que l'« étude » n'avait jamais été

formulée par écrit et n'était fondée que sur la consultation verbale d'un expert. Après avoir examiné les faits, le CEPD a conclu que rien ne prouvait l'existence de l'étude et que, par conséquent, les données à caractère personnel n'existaient pas et qu'il n'était donc pas possible d'y avoir accès.

### Traitement de données sensibles

Un ancien membre du personnel de la Commission a adressé au CEPD une réclamation 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 de l'assurance accidents (dossier 2007 0521). L'auteur de la réclamation estimait que cette catégorie particulière de données à caractère personnel au sens de l'article 10, paragraphe 1, du règlement avait été transférée à un tiers sans que la nécessité de ce traitement ne soit suffisamment étayée conformément à l'article 10, paragraphe 2, point b). La Commission a effectivement transféré des informations relatives à l'« expertise psychiatrique » de la personne concernée. Après avoir examiné les faits, le CEPD a conclu que la Commission n'était pas fondée à divulguer cette expertise spécifique.

Une autre réclamation a été adressée par un membre du personnel de la Commission concernant le traitement de données à caractère personnel se rapportant à sa vie sexuelle (dossier 2007 459). L'auteur de la réclamation s'est également plaint de la divulgation de ces données à des tiers. Après avoir enquêté, le CEPD a conclu :

- que les données à caractère personnel de l'auteur de la réclamation avaient fait l'objet d'un traitement sans base juridique ;
- que l'auteur de la réclamation n'avait pas reçu les informations nécessaires concernant le traitement (ou n'avait pas été averti des raisons justifiant le report de leur communication) ;
- que les mesures de sécurité applicables n'avaient pas été appropriées au regard des risques présentés par le traitement et de la nature des données à caractère personnel.

En outre, le CEPD a invité les services concernés de la Commission à mettre en œuvre des mesures visant à prévenir à l'avenir toute violation du règlement (CE) n° 45/2001. À la suite de la décision du CEPD, la Commission s'est engagée à prendre les mesures voulues pour se conformer aux dispositions du règlement.

Une réclamation a été introduite contre la Commission européenne dans le cadre d'une

procédure d'attribution des places de parking réservées aux membres du personnel handicapés (dossier 2007 611). Un membre du personnel de la Commission s'est plaint de ce que des données sensibles relatives à sa santé aient été envoyées par courrier électronique à différents tiers sans raison manifeste. Après avoir examiné les faits, le CEPD a conclu qu'il existait une base juridique permettant la transmission du courrier électronique aux autres personnes afin qu'elles soient en mesure de se prononcer sur la prolongation de l'attribution de la place de parking, mais que les données médicales auraient dû être supprimées du courriel adressé à certains des destinataires. Le CEPD a saisi le responsable du traitement et a demandé que les données médicales soient supprimées par les destinataires qui les avaient reçues sans raison valable.

Une autre réclamation portait sur la violation présumée des droits à la protection des données dans le cadre de mesures prises à la suite d'une demande de congé spécial adressée par une personne désireuse de s'occuper d'un conjoint affecté d'une maladie grave (dossier 2007 602). L'auteur de la réclamation a affirmé que le chef du personnel avait transmis ou, du moins, montré les deux certificats médicaux à l'autorité investie du pouvoir de nomination (AIPN), en violation de l'article 10, paragraphe 3, du règlement.

Après avoir déclaré la réclamation recevable, le CEPD a centré sa décision sur le fait que des données relatives à la santé avaient été transmises à l'AIPN sans le consentement de la personne concernée et sans que cette transmission soit fondée sur le traité CE ou un acte juridique adopté sur la base des traités, en violation de l'article 10, paragraphe 3, du règlement.

Les dispositions régissant les congés prévoient bel et bien que, dans le cadre d'une demande de congé spécial non supérieur à trois jours, un certificat médical doit, en principe, être fourni au gestionnaire des congés. Il n'est toutefois pas prévu que le certificat médical puisse être transmis à l'AIPN. En réalité, l'intervention de l'AIPN n'est explicitement prévue que dans les cas de maladie chronique grave, lorsqu'elle peut être amenée à accorder des prolongations ne dépassant pas trois jours. En outre, selon les dispositions précitées, si la personne estime que les informations figurant dans le certificat sont confidentielles, le certificat ne peut être communiqué qu'au service médical et le gestionnaire des congés ne recevra que les informations de base relatives au congé. Cette disposition exclut donc expressément la communication de données confidentielles

au gestionnaire des congés et, *a fortiori*, à l'AIPN. En l'absence de service médical dans l'organisme concerné, l'auteur de la réclamation avait transmis le certificat médical au responsable des ressources humaines en demandant explicitement la confidentialité. La communication ultérieure de ces données à l'AIPN ne pouvait donc pas se justifier sur la base des dispositions d'application.

Le CEPD a également fait observer que la procédure de demande d'un congé spécial devrait lui être soumise pour contrôle préalable puisque cette procédure suppose le traitement de données relatives à la santé.

Dans un autre dossier, l'auteur de la réclamation a affirmé que le traitement de certaines de ses données dans le cadre de la procédure d'évaluation mise en place dans une agence constituait une violation de l'article 10 du règlement (dossier 2008-124). Les données traitées par son notateur dans le cadre de l'exercice d'évaluation concernaient la santé de l'auteur de la réclamation (nombre de jours de congé maladie), les activités professionnelles de son conjoint et le fait qu'il était un membre actif du comité du personnel.

S'agissant des données relatives à la santé, le CEPD a considéré qu'elles étaient pertinentes dans la mesure où elles étaient nécessaires pour rendre compte du temps de travail réel dans la perspective de l'évaluation de la personne concernée. Pour ce qui était des données relatives aux activités professionnelles du conjoint de l'auteur de la réclamation, le CEPD a fait observer que ces informations n'étaient pas pertinentes au regard de la protection des données. Pour ce qui était de l'appartenance de la personne concernée au comité du personnel, le CEPD a estimé que ces données n'étaient pas couvertes par l'article 10, paragraphe 1, du règlement, qui mentionne explicitement l'interdiction de traitement des données à caractère personnel qui révèlent l'appartenance syndicale et n'évoque pas l'interdiction de celles relatives à l'appartenance à un comité du personnel. Il a également été fait observer que ces données étaient pertinentes et non excessives au regard des finalités de l'exercice d'évaluation car le temps consacré aux activités en question fait partie du temps de travail, ce qui est donc conforme aux dispositions de l'article 4, paragraphe 1, point c), du règlement.

#### **Droit de rectification**

Un fonctionnaire de la Commission européenne a adressé au CEPD une réclamation concernant le droit de rectification (dossier 2008-0353). L'auteur

de la réclamation avait envoyé plusieurs demandes à différents services de la Commission afin d'obtenir une rectification de ses données à caractère personnel relatives à Flexitime dans le système Sysper2. La Commission n'avait pas réagi à ces demandes. Après l'introduction de cette réclamation auprès du CEPD, la DG Personnel et administration a finalement rectifié les données incorrectes dans le dossier concerné.

### Obligation d'information

Une réclamation a été introduite contre la Commission européenne dans le cadre d'un traitement de données concernant l'assurance accidents (dossier 2007 0520). L'auteur de la réclamation a déclaré que des données le concernant et obtenues auprès de lui et de tiers avaient été collectées, conservées et transférées à des tiers sans qu'il en soit dûment informé (articles 11 et 12 du règlement). La personne en question se plaignait également de ce qu'elle n'avait pas eu accès à l'ensemble des données la concernant traitées par la Commission. Par ailleurs, l'auteur de la réclamation a déclaré qu'il estimait que la Commission avait donné une présentation sélective et tendancieuse de son dossier, et qu'il souhaitait donc exercer son droit de rectification (article 14 du règlement).

Après avoir examiné ce dossier, le CEPD a conclu que le responsable du traitement n'avait pas respecté les obligations qui lui incombent en vertu des articles 11 et 12 du règlement, et il a rejeté la réclamation pour d'autres motifs.

Le CEPD a reçu une autre réclamation, introduite par un ancien membre du personnel de l'Agence européenne pour l'environnement (AEE), faisant état d'une violation supposée du règlement (CE) n° 45/2001 par l'agence, en l'occurrence un transfert illicite et excessif de données financières détaillées le concernant entre deux destinataires au sein de l'agence (dossier 2007 0718).

Après avoir procédé aux enquêtes nécessaires, le CEPD a estimé que, même si le transfert des données financières de l'auteur de la réclamation était nécessaire à la planification budgétaire d'un projet, l'agence ne l'avait pas informé de ses droits à l'égard du transfert avant que ce dernier n'ait lieu, contrairement à ce que prévoit l'article 12 du règlement. Dans sa décision, le CEPD a donc recommandé que l'agence mette en œuvre des règles spécifiques aux transferts au sein de l'agence, à la conservation des données transférées et aux informations à fournir aux personnes concernées.

### Présentation d'un dossier dans le rapport annuel 2005 – Nouvelle mise à jour

En juillet 2005, le CEPD a reçu une réclamation contre l'OLAF soulevant plusieurs questions relevant du règlement (CE) n° 45/2001, notamment le traitement déloyal de données à caractère personnel et le transfert de données erronées concernant l'auteur de la réclamation 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).

En décembre 2005, le CEPD adjoint a adopté une décision concernant cette réclamation. Il a certes reconnu que le CEPD était compétent pour entendre cette réclamation, dans la mesure où elle soulève des questions relevant du règlement, mais il a conclu que le CEPD ne pouvait pas prendre d'autres mesures, qui modifieraient la situation à l'avantage de l'auteur de la réclamation. Ce dossier a été brièvement évoqué dans le rapport annuel 2005.

En 2006, l'auteur de la réclamation a saisi le médiateur européen d'une plainte concernant la manière dont sa réclamation a été traitée. Dans une seconde 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 d'établir une mise à jour appropriée du dossier, comprenant une description correcte et complète du dossier de l'auteur de la réclamation. Cette mise à jour a été publiée dans le rapport annuel 2007. De plus, à la lumière de la décision prise par le médiateur concernant la deuxième plainte, une note correspondante a été ajoutée au rapport annuel 2005 disponible sur le site web du CEPD.

S'agissant de la première plainte, le médiateur a conclu en avril 2008 qu'il ne serait pas justifié d'effectuer d'autres enquêtes concernant les affirmations de l'auteur de la réclamation et il a donc clôturé le dossier. Dans une autre observation, il a admis que, au vu de l'article 46, points a) et b), du règlement (CE) n° 45/2001, le CEPD bénéficiait bien d'une certaine marge d'appréciation pour déterminer les plaintes qui devraient donner lieu à une enquête. Le médiateur a aussi estimé qu'il serait judicieux et très utile pour les personnes qui seraient amenées à introduire des plaintes à l'avenir que le CEPD indique, dans un document d'orientation générale, les critères ou les lignes directrices qu'il compte appliquer lorsqu'il exercera son pouvoir d'appréciation pour déterminer s'il convient d'ouvrir une enquête

à la suite d'une réclamation introduite auprès de lui. Dans le prolongement de ce qui précède, un manuel interne sur le traitement des plaintes sera élaboré et des informations sur les principaux éléments de la procédure, ainsi que des informations sur la recevabilité des plaintes seront publiées ultérieurement sur le site web du CEPD (voir section 2.4.5).

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

Sur les 91 plaintes reçues en 2008, 68 ont été déclarées irrecevables. 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 si un État membre ne devait pas appliquer de manière correcte les dispositions de la directive 95/46/CE.

#### Institutions et organes communautaires non directement concernés

À titre d'exemple, le CEPD a reçu deux plaintes portant sur le traitement de données à caractère personnel concernant des membres du personnel des CE alors que le traitement n'était pas effectué par une institution ou un organe communautaire mais bien par les syndicats œuvrant au sein de ces institutions. C'était le cas, par exemple, d'un membre du personnel se plaignant d'avoir reçu, à son adresse électronique professionnelle, des informations à caractère politique transmises par un syndicat. En l'occurrence, le syndicat s'était servi de la liste de toutes les adresses électroniques fournies par l'institution. La réclamation concernait cependant l'utilisation de ces informations par un syndicat agissant en vertu de la loi nationale (dossier 2008-724). Un autre exemple concernait la divulgation de données à caractère personnel à des tiers par le syndicat d'un membre du personnel des CE. En l'espèce également, le CEPD a conclu que le règlement (CE) n° 45/2001 n'était pas applicable, le syndicat concerné étant une personne morale relevant du droit national (affaire 2008 071). Les coordonnées des autorités nationales de protection des données ont donc été fournies, assorties d'une explication sur les raisons pour lesquelles le CEPD n'était pas compétent pour traiter le dossier.

#### Violations n'ayant pas trait au traitement de données à caractère personnel

De nombreuses plaintes ont notamment été déclarées non recevables parce qu'elles portaient sur des violations qui auraient été commises par des institutions ou des organes communautaires alors que ces cas ne ressortissaient pas du champ d'application du règlement (CE) n° 45/2001. En fait, certains auteurs de réclamation essayaient de faire réviser ou annuler des décisions de l'administration communautaire en faisant valoir que ces décisions contenaient des données à caractère personnel et qu'il fallait respecter leur droit de rectification de telles données.

Le CEPD a déclaré ces plaintes irrecevables au motif que, même si une décision de l'administration communautaire contient des données à caractère personnel, cela ne signifie pas que le CEPD soit compétent pour enquêter à la suite d'une réclamation introduite contre une décision de cette nature. Pour être recevable, la réclamation doit porter sur le traitement de données à caractère personnel en tant que telles et non sur l'interprétation de la notion de données à caractère personnel lorsqu'une institution exerce son pouvoir d'appréciation.

#### Les mêmes faits sont déjà examinés par d'autres instances

Le CEPD déclare normalement une réclamation irrecevable si les mêmes faits (circonstances factuelles identiques) ont déjà fait l'objet d'un examen de la part d'une juridiction, du médiateur européen ou d'une instance administrative analogue. C'était le cas, par exemple, d'un membre du personnel se plaignant de la non application du règlement (CE) n° 45/2001 dans le cadre d'une enquête administrative effectuée par un organe communautaire. Cette enquête administrative avait été entreprise en vue d'établir les faits concernant un litige relatif à un supposé accès non autorisé à la boîte aux lettres électronique de l'auteur de la réclamation. L'enquête administrative a été suivie d'une procédure disciplinaire, qui était toujours en cours au moment de l'introduction de la réclamation. En outre, l'auteur de la réclamation avait saisi le médiateur européen d'une plainte analogue.

Selon le CEPD, il serait prématuré de statuer sur la question de la non application du règlement tant que l'administration n'aura pas rendu ses conclusions définitives sur le sujet dans le cadre de l'enquête disciplinaire. L'examen du dossier par le CEPD donnerait également lieu à une multiplication des procédures avec le médiateur européen.

#### 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/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.

Le médiateur 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 réclamation 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.

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

Le CEPD a poursuivi l'établissement d'un manuel interne relatif au traitement des plaintes par ses services. Les principaux éléments de la procédure, un formulaire-type pour l'introduction des plaintes et des informations relatives à la recevabilité des plaintes seront disponibles sur le site web du CEPD en 2009. Cette publication devrait aider les éventuels auteurs de plaintes à présenter celles-ci, tout en réduisant le nombre de plaintes manifestement irrecevables et en donnant au CEPD les informations les plus complètes et les plus pertinentes susceptibles de faciliter le traitement des réclamations.

## 2.5. Politique d'inspection

### 2.5.1. 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 appelée « printemps 2007 » dans le cadre d'une initiative visant à évaluer le respect du règlement au sein des institutions et agences et à faire le point sur les progrès accomplis.

La première partie de la procédure lancée en 2007 a pris la forme de lettres adressées aux directeurs des institutions et des organes afin d'évaluer le niveau de conformité au règlement. Quatre catégories de questions ont été posées concernant : le statut du délégué à la protection des données (DPD) ; l'inventaire des traitements portant sur des données à caractère personnel ; l'inventaire des traitements relevant de l'article 27 du règlement et la poursuite de la mise en œuvre du règlement proprement dit. Cette procédure a obligé les organes qui ne l'avaient pas encore fait à désigner un DPD et à étudier la question des ressources et du personnel nécessaires à l'exercice de ses fonctions. Elle a également encouragé les institutions et organes à recenser 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 en 2007.

Sur la base des informations transmises en retour par les institutions et les organes, le CEPD a établi un rapport général sur le niveau de conformité. Ce rapport a été publié en mai 2008 et envoyé à l'ensemble des institutions et organes.

Comme cela avait été annoncé, la procédure a été 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. Concernant ce dernier point, des lettres ont été envoyées en octobre 2008 pour demander de nouvelles mises à jour sur la situation dans les organes et les institutions. D'autres questions ont également été soulevées concernant la poursuite de la mise en œuvre du règlement, notamment pour ce qui est de l'exercice des droits de la personne

concernée et le niveau des plaintes introduites auprès des DPD. Les réponses à ces questions étaient attendues en décembre 2008 ; elles donneront lieu à un nouveau rapport au cours du printemps 2009.

### 2.5.2. Inspections

Le CEPD a récemment commencé à développer sa politique d'inspection. L'expérience précédemment acquise lors des enquêtes effectuées dans le cadre d'une réclamation et la procédure « printemps 2007 » ont rendu nécessaire la systématisation des activités d'inspection du CEPD en vertu des pouvoirs conférés au Contrôleur par différents articles du règlement (CE) n° 45/2001.

Les inspections constituent un outil indispensable pour que le CEPD en qualité d'autorité de contrôle puisse surveiller et assurer l'application des dispositions du règlement (article 41, paragraphe 2, et article 46, point c)). Les pouvoirs étendus qui sont conférés au CEPD pour avoir accès à toutes les informations et données à caractère personnel nécessaires à ses enquêtes et obtenir l'accès à tous les locaux dans lesquels un responsable du traitement ou une institution ou un organe communautaire exerce ses activités ont pour objet de lui permettre de disposer de moyens efficaces pour s'acquitter de ses fonctions publiques (article 47, paragraphe 2, du règlement). Les inspections peuvent résulter d'une réclamation ou être effectuées de la propre initiative du CEPD (article 46, points a) et b), du règlement).

Les institutions et organes européens sont tenus de coopérer avec le CEPD dans l'accomplissement de ses fonctions et devraient communiquer les informations demandées et accorder l'accès requis (article 30 du règlement).

Au cours des inspections, le CEPD vérifie les faits et la réalité sur place, son objectif étant également de s'assurer que les institutions et organes communautaires se conforment au règlement. En outre, les inspections peuvent contribuer dans une large mesure à accroître la sensibilisation aux questions relatives à la protection des données dans les institutions qui en font l'objet et elles peuvent également faciliter le travail des délégués à la protection des données.

En 2008, le CEPD a défini la première procédure globale concernant ses activités d'inspection dans le domaine du contrôle. Cette procédure a comporté trois phases :

- au cours de la première phase, deux visites « de répétition » ont été réalisées pour tester la méthode du CEPD sur place ;

- au cours de la deuxième phase, le CEPD a perfectionné sa méthode pratique ;
- au cours de la troisième phase, deux inspections ont été réalisées dans des institutions européennes qui avaient été sélectionnées dans le cadre de l'exercice « printemps 2007 ».

### Visites de « répétition »

L'objectif général de ces visites effectuées sur place était double : outre le fait de tester la méthode d'inspection du CEPD, il s'agissait de vérifier si le règlement était réellement respecté dans des domaines précis. Cela signifie que le CEPD a formulé des recommandations dans un nombre appréciable de cas pour améliorer le niveau de protection des données dans les services ayant fait l'objet d'une visite. Pour ces cas, les responsables du traitement étaient censés communiquer des informations en retour dans un délai déterminé.

#### *Conseil de l'Union européenne*

En juillet 2008, trois visites ont été effectuées dans les locaux du Conseil de l'Union européenne (dossier 2008-359). Pour le CEPD, ces visites avaient pour objectif de perfectionner davantage sa méthode pratique en matière d'inspections mais elles lui ont aussi permis de vérifier deux traitements de données à caractère personnel et de procéder à des entretiens dans une direction.

Durant la première visite, le CEPD a vérifié certains éléments de la notification transmise au DPD (extraite du registre de ce dernier) concernant le traitement de données à caractère personnel dans le cadre de la fixation des droits à l'entrée en fonctions. Le CEPD a délivré des recommandations à la suite de la visite et le responsable du traitement l'a déjà informé des mesures prises.

La visite suivante, qui a eu lieu à la direction des systèmes d'information et de communication, avait pour objectif de vérifier la nature des mesures mises en place par le responsable du traitement pour que les traitements de données à caractère personnel soient notifiés au DPD (article 25 du règlement). Le CEPD assurera un suivi des progrès accomplis dans ce domaine et il a demandé des informations en retour sur la désignation d'un point de contact dans la direction pour les questions de protection des données et sur le statut des notifications.

La troisième visite s'est articulée autour d'un traitement qui avait déjà fait l'objet d'un contrôle préalable de la part du CEPD. Ses services ont vérifié les

traitements de données à caractère personnel liés à la procédure de sélection des stagiaires (dossier 2007-217) et la mise en œuvre de ses recommandations. Le responsable du traitement a déjà transmis au CEPD des informations sur la mise en œuvre de certaines des recommandations qu'il avait formulées à l'issue de la visite. Quelques questions restent néanmoins en suspens.

#### *OLAF*

En octobre 2008, les services du CEPD ont effectué une visite dans les locaux de l'OLAF en vue de perfectionner encore la méthode pratique du CEPD en matière d'inspections. Il s'agissait également de procéder à un examen objectif des mesures prises par l'OLAF pour garantir la mise en œuvre de certaines recommandations présentées dans un avis de contrôle préalable rendu par le CEPD concernant les enquêtes internes de l'Office (dossier 2005-418).

Lors de sa visite (dossier 2008-488), le CEPD a principalement porté son attention sur quelques éléments importants au regard de la protection des données, notamment la pratique consistant à identifier certaines catégories de personnes concernées dans l'onglet relatif aux personnes du système de gestion des dossiers (CMS) de l'OLAF. Les services du CEPD ont également eu accès à certains dossiers de l'OLAF dans le CMS afin d'examiner les notes d'information envoyées aux personnes concernées, la pratique de report de l'obligation d'information et les transferts de données à caractère personnel se rapportant aux dossiers sélectionnés pour la visite. Par ailleurs, le CEPD a enquêté sur les notifications qu'il est prévu de transmettre au DPD de l'OLAF lorsque des courriers électroniques ou des documents de nature personnelle sont concernés dans le cadre du protocole de procédures opératoires normalisées pour la réalisation d'analyses criminalistiques d'ordinateurs.

Dans les informations qu'il a transmises à l'OLAF après sa visite, le CEPD a insisté sur son approche antérieure dans les domaines examinés. L'obligation d'information devrait être mise en œuvre et une note devrait être conservée dans le dossier en cas de report de l'information. Des notes devraient être transmises lorsqu'un transfert de données à caractère personnel intervient. Le CEPD a encouragé l'OLAF à régler la pratique des transferts verbaux. Il a invité l'OLAF à se servir de l'onglet relatif aux personnes qui est utilisé pour identifier les personnes concernées dans le CMS comme d'un outil utile permettant de mettre en œuvre correctement d'autres obligations.

Étant donné que le protocole de l'OLAF relatif aux analyses criminalistiques d'ordinateurs n'est toujours qu'un projet, le CEPD a encouragé l'Office à prendre toutes les mesures nécessaires pour adopter le protocole en tant que document de l'OLAF et commencer à l'appliquer.

À titre d'observation générale, le CEPD a encouragé l'OLAF à établir des déclarations et/ou des notes normalisées concernant la protection des données afin de les mettre à la disposition des responsables des dossiers, qui pourraient les ajouter au texte des documents *ad hoc*. Il a également insisté sur la nécessité d'adopter les mesures nécessaires à la mise en application de tout le module de protection des données afin de mettre en œuvre les obligations visées dans le règlement (CE) n° 45/2001.

#### **Perfectionnement de la méthode pratique**

Les deux visites « de répétition » ont permis au CEPD de perfectionner son manuel des inspections internes et d'établir la version actuelle des lignes directrices sur la politique d'inspection.

Le manuel des inspections constitue un guide pratique destiné aux membres des services du CEPD qui travaillent dans le domaine du contrôle et qui sont membres d'une équipe d'inspection. Il contient la description de la procédure administrative et des tâches du personnel chargé des inspections, des formulaires normalisés pour l'établissement des documents d'inspection et la politique de sécurité en matière d'inspection. Il explique les finalités de ces documents et il donne des conseils utiles pour préparer une inspection. La version actuelle du manuel peut faire l'objet de modifications, les pratiques du CEPD évoluant en fonction de l'expérience. Le manuel, qui sera formellement adopté en 2009, sera révisé et, au besoin, actualisé chaque année.

La version actuelle des lignes directrices sur la politique d'inspection est envoyée aux institutions et organes avant que l'inspection n'ait lieu. Une fois mises au point, les lignes directrices seront publiées sur le site web du CEPD. Elles décrivent notamment les étapes principales d'une procédure d'inspection, la base juridique des inspections, les compétences du CEPD et le rôle des DPD durant une inspection.

#### **Inspections liées à l'exercice « printemps 2007 »**

En mai 2008, le CEPD a décidé de procéder à une inspection dans trois institutions et un organe, essentiellement sur la base des constatations faites

dans le cadre de l'exercice « printemps 2007 ». Deux inspections ont été effectuées, en novembre et décembre 2008 respectivement, et deux autres sont prévues pour le début de 2009.

#### *Comité économique et social européen*

En novembre 2008, le CEPD a procédé à une inspection au Comité économique et social européen (CESE) (dossier 2008 574). L'inspection a été effectuée pour procéder à un examen objectif des mesures prises par le comité pour se conformer au règlement dans deux domaines essentiels :

- la situation de l'inventaire du DPD et l'obligation faite aux responsables des traitements de notifier les traitements de données à caractère personnel au DPD (article 25 du règlement) ;
- le traitement de données concernant la gestion des demandes de stage rémunéré (dossier 2005-297) et le traitement de données à caractère personnel par le service médical (dossier 2007-0004). Les deux traitements avaient déjà fait l'objet antérieurement d'un contrôle préalable du CEPD, qui avait formulé des recommandations afin que les responsables du traitement renforcent le niveau de protection des données à caractère personnel.

*Inventaire et notifications* : les responsables de traitement qui n'avaient pas encore transmis au DPD la notification finale des traitements de données effectués jusqu'alors se sont entretenus avec le personnel du CEPD chargé de l'inspection pour expliquer les raisons de cette situation, les mesures mises en place pour permettre des progrès dans ce domaine et les délais prévus en vue de la notification au DPD.

*Gestion des demandes de stage rémunéré* : le personnel du CEPD chargé de l'inspection a procédé à la vérification et à l'observation d'un certain nombre d'éléments tant dans la demande électronique que dans les dossiers papier, notamment les documents (informations) collectés auprès des candidats aux différents stades de la procédure de demande, les informations traitées dans la demande électronique, les pratiques en matière de conservation des données, les mesures de sécurité appliquées aux dossiers papier, les informations demandées sur le rôle du conseiller de stage et sur son accès aux informations et les informations demandées sur la déclaration relative au respect de la vie privée.

*Traitement des données effectué par le service médical du CESE* : le personnel chargé de l'inspection a notamment examiné les pratiques en vigueur au service médical du CESE après la séparation des

services médicaux du CESE et du CdR, contrôlé les mesures de sécurité applicables aux dossiers papier, demandé des informations sur l'obligation de secret professionnel incombant aux membres du personnel autres que les médecins, contrôlé les éventuelles informations relatives à la santé que le médecin du CESE peut recevoir dans les cas où un membre du personnel décide de consulter un médecin de son choix, et posé des questions sur les pratiques en matière de transmission des notes d'honoraires, de droit d'accès des personnes aux données les concernant et d'information des personnes concernées.

Le CEPD a transmis des remarques détaillées à l'issue de l'inspection et demandé que de nouveaux progrès soient accomplis dans certains des domaines inspectés.

#### *Autorité européenne de sécurité des aliments*

En décembre 2008, les services du CEPD ont effectué une inspection dans les locaux de l'Agence européenne de sécurité des aliments (AESA) (dossier 2008 575). Il s'agissait de vérifier les mesures prises par l'AESA pour se conformer au règlement dans les domaines essentiels suivants :

- l'obligation faite aux responsables des traitements de notifier les traitements de données à caractère personnel au délégué à la protection des données (DPD) (article 25 du règlement) ;
- contrôle d'un traitement de données à caractère personnel concernant la politique de formation du personnel qui a été inventorié mais pas encore notifié ;
- contrôle de la mise en œuvre des recommandations que le CEPD avait formulées dans son avis de contrôle préalable relatif à la « procédure d'évaluation du personnel et d'évolution de carrière » (dossier 2007 585) (article 27 du règlement).

En lien avec l'exercice « printemps 2007 », le CEPD a également procédé à une enquête sur l'augmentation en pourcentage du temps de travail du DPD et de ses services administratifs ou de secrétariat.

Les conclusions de l'inspection seront communiquées à l'AESA au début de 2009.

#### **Conclusions**

Au cours de ces inspections, le CEPD s'est focalisé sur différents aspects, notamment le contrôle de la situation de l'inventaire du DPD et des notifications qui lui ont été transmises (un élément requis

durant l'exercice « printemps 2007 ») et le traitement spécifique extrait de l'inventaire ou du registre du DPD, ainsi que la vérification du suivi donné concrètement aux recommandations formulées par le CEPD dans ses avis de contrôle préalable.

Les premières expériences acquises en la matière montrent que les inspections constituent un outil utile non seulement pour contrôler la situation réelle dans les institutions et organes communautaires mais aussi pour servir de moyen de sensibilisation. Le CEPD a profité de ces inspections pour rencontrer différents responsables de traitement et leur expliquer les obligations qui leur incombent en vertu du règlement (CE) n° 45/2001. Les entretiens réalisés avec différents intervenants et l'évaluation des progrès accomplis ont montré clairement au CEPD quel était le niveau de coopération entre les responsables de traitement et les DPD. À cet égard, les inspections peuvent aussi être perçues comme un moyen de faciliter le travail des DPD.

## 2.6. Mesures administratives

L'article 28, paragraphe 1, du règlement (CE) n° 45/2001 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 de l'institution ou de l'organe concerné, soit de sa propre initiative. Une « mesure administrative » doit s'entendre comme une décision de l'administration d'application générale qui se rapporte au traitement de données à caractère personnel effectué par l'institution ou l'organe concerné. Il pourrait s'agir de modalités d'application du règlement, ou de règles internes ou encore d'orientations d'application générale adoptées par l'administration dans le cadre du traitement de données à caractère personnel.

Par ailleurs, l'article 46, point d), du règlement prévoit un champ d'application matériel très large pour les consultations, en ce sens qu'il les étend à « toutes les questions concernant le traitement de données à caractère personnel ». C'est la base sur laquelle le CEPD s'appuie pour conseiller les institutions et organes communautaires sur des dossiers particuliers supposant des traitements ou sur des questions abstraites relatives à l'interprétation du règlement.

Dans le cadre de consultations menées sur des mesures administratives <sup>(19)</sup> envisagées par les institutions ou organes communautaires, plusieurs questions délicates ont été soulevées, notamment par exemple :

- un nouvel modèle de certificat médical ;
- l'accès aux documents contenant des données à caractère personnel ;
- la loi applicable à certains traitements ;
- le transfert d'un dossier médical à une jurisprudence nationale ;
- la conservation d'informations relatives à des sanctions disciplinaires dans le cadre de la protection des données ;
- les dispositions d'application du règlement (CE) n° 45/2001 adoptées par la Cour de justice ;
- les plaintes traitées par le médiateur européen.

### 2.6.1. Nouvel modèle de certificat médical

Le Collège médical interinstitutionnel a présenté au CEPD un projet de nouveau modèle de certificat d'incapacité de travail pour maladie ou accident. L'objectif est de simplifier et de moderniser le service médical de la Commission et d'offrir des facilités au personnel (en l'occurrence, le nouveau certificat sera disponible sur l'intranet pour être utilisé s'il y a lieu en cas de consultation d'un médecin).

Le CEPD a notamment recommandé que le teneur des données médicales que le projet de certificat devrait contenir soit réexaminée à la lumière des principes du caractère adéquat et de la pertinence. Il a en outre préconisé qu'une note d'information soit établie pour donner des informations spécifiques sur le traitement et des informations exhaustives sur les droits d'accès et de rectification et sur la conservation des données, conformément aux articles 11 et 12 du règlement. Ces informations devraient également figurer au verso du certificat médical afin que les patients comme les médecins soient au courant de leurs droits (dossier 2008-312).

### 2.6.2. Accès aux documents

Le délégué à la protection des données (DPD) de la Commission européenne a présenté au CEPD une demande de consultation concernant une demande

<sup>(19)</sup> Même s'il existe des chevauchements et des différences entre les consultations effectuées en application de l'article 28, paragraphe 1, et celles effectuées en vertu de l'article 46, point d), on parlera dans les deux cas de « consultations menées sur des mesures administratives » dans le cadre du présent rapport.

d'accès à des documents contenant des données à caractère personnel, qui semblait pertinente dans le cadre d'un dossier pendant devant une juridiction nationale.

Dans un premier temps, la Commission a refusé de communiquer à l'auteur de la demande des informations sur la situation professionnelle d'un de ses employés ; en l'occurrence, il s'agissait de savoir si cette personne occupait un emploi à temps plein dans la DG concernée et si elle travaillait à la Commission à des moments bien précis.

La Commission a invoqué l'article 8 du règlement (CE) n° 45/2001 et soutenu :

- que l'auteur de la demande n'avait pas justifié la nécessité du transfert de ces données ;
- qu'il existait un risque de préjudice à l'égard de la personne concernée du fait qu'elle avait refusé de donner son consentement à la divulgation des informations et à une intervention dans la procédure.

Cela étant, la personne qui avait demandé un accès aux documents a introduit une plainte auprès du médiateur européen. Ce dernier a adopté une proposition de solution à l'amiable pour le dossier en suggérant que la Commission pourrait réexaminer son refus contesté et communiquer à l'auteur de la plainte les documents/informations demandés sans succès, sauf si elle invoque des motifs valides et adéquats pour ne pas le faire.

Étant donné que les informations demandées contenaient des données à caractère personnel, il a été examiné si l'exception prévue à l'article 4, paragraphe 1, point b), du règlement (CE) n° 1049/2001 était applicable. Le CEPD a suivi la méthode décrite dans son document de référence intitulé « Accès du public aux documents et protection des données »<sup>(20)</sup> afin d'évaluer si la vie privée de la personne serait affectée en l'espèce. Le CEPD a considéré qu'il n'avait pas reçu – et qu'il ne voyait pas – de raison valable de penser que la vie privée et l'intégrité de la personne concernée seraient en jeu et, en tout état de cause, que l'intérêt d'un accès du public aux documents ne prévaudrait pas en l'occurrence sur l'intérêt d'une protection des données de ladite personne. Par conséquent, le CEPD a estimé qu'il n'y avait pas de raison de refuser un tel accès sur la base de l'article 4, paragraphe 1, point b), du règlement (CE) n° 1049/2001 (dossier 2008 427).

<sup>(20)</sup> Juillet 2005, disponible sur le site [www.edps.europa.eu](http://www.edps.europa.eu). Voir en particulier la section 4.3.

### 2.6.3. Catégories de données particulières : législation applicable

Le DPD de l'Agence des droits fondamentaux de l'Union européenne a consulté le CEPD sur un traitement concernant une série de personnes intéressées dans les États membres de l'UE, qui souhaitaient participer à des enquêtes relatives aux droits fondamentaux, notamment dans le cadre de la discrimination et de la victimisation criminelle vécues par certains immigrants et d'autres groupes minoritaires. Un contrat été conclu entre l'agence et un contractant externe. L'un des objectifs du contrat était la collecte de catégories de données particulières, essentiellement de données révélant l'origine raciale ou ethnique. S'est posée la question de savoir si l'on pouvait invoquer une dérogation à l'article 10, paragraphe 1, du règlement (CE) n° 45/2001 afin d'éviter de devoir demander l'autorisation des autorités des États membres pour effectuer le traitement.

Le CEPD a expliqué que, la législation applicable au traitement analysé étant le règlement (CE) n° 45/2001 (l'agence est un organe européen et le traitement relève de l'article 3, paragraphe 2, du règlement), il n'est pas nécessaire de demander l'autorisation des autorités des États membres. Toutefois, la législation applicable aux obligations de confidentialité et de sécurité est le droit belge (lieu d'établissement du sous-traitant, ce dernier étant soumis à la loi nationale transposant la directive 95/46/CE). Ces obligations devraient donc figurer dans le contrat. En ce qui concerne la sensibilité des données, le CEPD a recommandé qu'une attention particulière soit accordée à la nature du consentement au sens de l'article 2, point h), du règlement. Il a été en outre recommandé d'établir une déclaration relative à la vie privée qui respecte strictement l'article 11 du règlement. Comme cela a été souligné, ce qui précède était également valable pour respecter l'obligation de recueillir un consentement « éclairé » (dossier 2008-331).

### 2.6.4. Demande émanant d'une juridiction en vue d'obtenir une copie du dossier médical complet d'un fonctionnaire

Le CEPD a été consulté par le DPD d'une agence dans le cadre d'une demande transmise par une juridiction au service médical de ladite agence en vue d'obtenir une copie du dossier médical complet d'un fonctionnaire aux fins d'une procédure de divorce.

Le CEPD a estimé que, dans le dossier analysé, le responsable du traitement était soumis à l'obligation de coopérer avec les juridictions nationales et que le traitement serait par conséquent justifié de ce point de vue (compte tenu de l'article 5, point b), du règlement qui indique que le traitement de données à caractère personnel ne peut être effectué que si « le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »). Toutefois, le service médical est soumis aux obligations découlant des règles régissant le secret médical. Par voie de conséquence, la coopération avec les juridictions nationales doit intervenir dans le respect des obligations et mécanismes instaurés par les règles nationales régissant le secret médical lorsque des informations sont demandées par des juridictions dans le cadre de procédures judiciaires.

Le CEPD a fait observer que, compte tenu de la sensibilité de la catégorie de données concernée, il serait recommandé d'obtenir le consentement de la personne concernée pour conforter la licéité du traitement (article 5, point d), du règlement). Toutefois, le refus de consentement opposé par la personne concernée n'invaliderait pas la base fondée sur l'article 5, point b), comme expliqué plus haut. En tout état de cause, un refus de donner le consentement doit être pris en compte du point de vue de la proportionnalité et la qualité des données en général.

Le CEPD a en outre souligné que, avant le transfert du dossier médical, le responsable du traitement

devait s'assurer que seules les données adéquates, pertinentes et non excessives allaient être transférées. Étant donné que la demande de la juridiction ne précisait pas la finalité du traitement demandé, il était légitime, au regard de l'article 4, paragraphe 1, point b), de demander des précisions supplémentaires à ce propos (dossier 2008-145).

### 2.6.5. Conservation des informations relatives à des sanctions disciplinaires dans le cadre de la protection des données

Le CEPD a fait connaître au président du collège des chefs d'administration sa position concernant les délais de conservation, dans les dossiers disciplinaires, des données relatives aux sanctions après que celles-ci ont été exécutées. Il a souligné le manque de compatibilité entre l'interprétation actuelle du statut et les droits fondamentaux, notamment pour ce qui est de la protection des données.

Plus particulièrement, le CEPD a souligné que, en tout premier lieu, l'article 27 de l'annexe IX du statut s'opposait au règlement (CE) n° 45/2001 du fait que la règle énonce que la décision de suppression est laissée à l'appréciation de l'autorité investie du pouvoir de nomination. Par contre, le règlement exige notamment que les données soient conservées « pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles

elles sont traitées ultérieurement ». Par voie de conséquence, dans ce contexte, le CEPD a estimé que, lors d'une future révision du statut, il serait souhaitable de réexaminer au vu de ce qui précède les délais en vigueur et de rendre obligatoire la suppression de toutes les mentions de mesures disciplinaires après l'expiration des délais fixés.

Deuxièmement, le CEPD a considéré qu'une interprétation correcte de l'article 10, points h) et i), ne devrait pas être en contradiction avec la véritable finalité de l'article 27. Par conséquent, le



Avant de transférer un dossier médical à un tribunal, le responsable du traitement doit veiller au respect du principe de la qualité des données.

premier doit être lu « sans préjudice » du second, et non l'inverse, de façon à éviter toute atteinte aux droits fondamentaux des membres du personnel.

Troisièmement, il convient que les dossiers disciplinaires ne soient pas conservés indéfiniment, même après que la mention de la sanction ait été effacée du dossier individuel. Il ne s'agit pas seulement d'une violation de l'article 4, paragraphe 1, point e), du règlement mais aussi d'une atteinte au principe de non conservation de dossiers parallèles conformément à la jurisprudence du Tribunal de première instance.

Quatrièmement, le CEPD a fait observer que l'article 13 de l'annexe IX utilise la formule « dossier individuel » au sens de « dossier disciplinaire de la personne ». Toute autre interprétation n'apporterait rien à l'article 26 du statut et viderait de sens l'article 13, notamment au regard du droit dont bénéficient les membres du personnel en vertu de l'article 41, paragraphe 2, point b), de la Charte des droits fondamentaux de l'UE (dossier 2006 075).

#### **2.6.6. Dispositions d'application du règlement (CE) n° 45/2001**

Le délégué à la protection des données (DPD) de la Cour de justice des Communautés européennes a présenté au CEPD une demande de consultation concernant un projet de décision du comité administratif de la Cour de justice sur les dispositions d'application du règlement (CE) n° 45/2001. Le projet ne concernait que des aspects liés à l'article 24, paragraphe 8, et l'annexe du règlement (tâches et obligations des DPD et des responsables des traitements) et non des aspects relatifs aux personnes concernées, couverts par d'autres modalités d'application. Dans le cadre de ce champ d'application limité, certaines dispositions manquantes ont été relevées, concernant notamment la durée du mandat du DPD et son évaluation. Il a aussi été conseillé d'élargir quelque peu la portée des enquêtes du DPD. Le CEPD s'est néanmoins félicité du projet car il introduisait certaines bonnes pratiques qu'il encourage, notamment les liens entre le DPD et les services informatiques de la Cour (dossier 2008 0658).

#### **2.6.7. Plaintes traitées par le médiateur européen**

Le CEPD a conseillé le médiateur européen sur les incidences qu'entraîne du point de vue de la

protection des données la transmission aux institutions communautaires concernées des décisions du médiateur de ne pas ouvrir d'enquête suite à une plainte donnée et des raisons motivant ces décisions (dossier 2008 608). Dans ce cas particulier et sachant que la règle par défaut en vigueur au bureau du médiateur est le traitement public des plaintes, le CEPD a recommandé que le plaignant soit informé que, pour autant qu'il n'ait pas déjà choisi la confidentialité, si sa plainte est déclarée irrecevable, il peut de nouveau choisir la confidentialité après avoir reçu la décision.

## **2.7. Vidéosurveillance**

### **2.7.1. Lignes directrices**

En 2008, 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 de l'UE des orientations pratiques sur le respect des règles de protection des données lors de l'utilisation de systèmes de vidéosurveillance. Le premier document de travail interne concernant le projet de lignes directrices a été établi à la fin de l'année. Le projet sera disponible pour consultation d'ici la mi-2009.

Il s'agit de donner des conseils pratiques plutôt que des notions théoriques juridiques. Ces lignes directrices doivent être flexibles mais elles sont aussi destinées à préciser les utilisations de données vidéo que le CEPD pourrait trouver critiquables, les mesures que les institutions doivent prendre avant d'installer un système de vidéosurveillance ou de mettre à jour un système existant et les mesures qu'elles doivent prendre de manière permanente pour que les questions de protection des données soient correctement prises en compte durant l'exploitation d'un système de vidéosurveillance.

Les lignes directrices recommandent aux institutions :

- d'établir clairement les objectifs qu'elles veulent atteindre au moyen du système ;
- d'évaluer soigneusement si la technique de la vidéosurveillance constitue un moyen efficace et proportionné pour atteindre ces objectifs ;
- de réfléchir aux solutions de substitution avant de décider un recours à des caméras ; et
- de collaborer avec le DPD de l'institution afin de déterminer l'endroit où les caméras seront instal-



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

lées, la manière de les utiliser et les garanties et limitations qui seront instaurées pour contribuer à protéger la vie privée des personnes filmées.

Les institutions sont également tenues de conserver les enregistrements vidéo pour une durée qui ne soit pas plus longue que nécessaire, de limiter strictement l'éventail des destinataires de ces enregistrements, de garder une trace de l'utilisation et du transfert des enregistrements vidéo et de prendre les mesures de sécurité adaptées afin de réduire au maximum le risque d'un accès non autorisé. En outre, les institutions doivent également informer le public de manière satisfaisante. Le CEPD préconise une approche multicouche de l'information, qui devrait comporter, outre des panneaux d'information installés sur place, des informations plus détaillées affichées sur le site web de l'institution. Chaque institution doit également créer un mécanisme pour répondre aux demandes d'accès émanant des personnes du public souhaitant savoir quelles sont les données vidéo les concernant qui font l'objet d'un traitement.

Les lignes directrices proposent des orientations détaillées aux institutions plus petites, notamment aux nombreux organes équipés d'un système de vidéosurveillance standard relativement simple.

### 2.7.2. Contrôles préalables

En 2008, le CEPD a également reçu deux autres notifications en vue d'un contrôle préalable *a*

*posteriori* concernant la vidéosurveillance, l'une émanant du CCR-IE de Petten et l'autre du CCR ITU de Karlsruhe. À l'instar des quatre notifications en vue d'un contrôle préalable *a posteriori* qui ont été reçues en 2007, 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 télévision en circuit fermé (CCTV) ont fait l'objet d'une procédure de contrôle préalable appropriée et ont été examinées

par le CEPD (dossier 2007-634). Cet avis rendu à la suite d'un contrôle préalable est le premier des avis du CEPD concernant la vidéosurveillance. Le dossier portait sur le système de CCTV exploité par l'OLAF dans ses locaux de Bruxelles à des fins de sécurité.

Dans l'ensemble, le CEPD a été satisfait de la proportionnalité du système de CCTV et des garanties mises en œuvre par l'OLAF pour assurer la protection des données. Les finalités du système sont clairement définies, relativement limitées et légitimes. De plus, l'emplacement, la zone couverte et la résolution, ainsi que d'autres aspects de la configuration du système de CCTV, semblent adéquats, pertinents et non excessifs au regard de la réalisation des finalités spécifiées, compte tenu également de la sensibilité des informations en possession de l'OLAF.

Le CEPD a néanmoins adressé d'importantes recommandations à l'OLAF en préconisant de reconsidérer les délais de conservation prévus afin que les données soient conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités initialement envisagées. Il a également recommandé que l'OLAF adopte un document interne décrivant son système de CCTV et prévoyant les garanties voulues en matière de protection des données. Enfin, le CEPD a aussi encouragé l'OLAF à donner des informations plus précises et correctes aux personnes concernées.

### 2.7.3. Plaintes

En 2008, le CEPD a continué d'assurer le suivi d'une réclamation introduite par un citoyen contre les pratiques du Parlement européen dans le domaine de la CCTV, plus particulièrement la surveillance effectuée à l'extérieur de ses bâtiments (dossier 2006-0185).

Des progrès ont été accomplis dans certains aspects importants du respect des règles de protection des données. Le Parlement a revu l'emplacement de ses caméras et, lorsqu'il a constaté que des zones privées de bâtiments adjacents se trouvaient dans leur champ de vision, il a pris des mesures techniques pour éviter ou réduire ce phénomène. Le Parlement a également accepté de donner aux personnes concernées des informations plus complètes sur ses pratiques en matière de CCTV, notamment par des avis sur son site web. Le Parlement conserve dorénavant un registre de tous les transferts d'enregistrements vidéo effectués par le service de sécurité vers d'autres destinataires appropriés tant à l'intérieur qu'à l'extérieur des institutions (par exemple tous les transferts à destination de la police sont maintenant inscrits dans le registre).

Cela étant, selon le CEPD, les mesures prises par le Parlement n'étaient pas entièrement satisfaisantes. Il aurait souhaité par exemple que les délais de conservation des enregistrements vidéo effectués à l'extérieur des locaux du Parlement soient beaucoup plus courts que ceux en vigueur. Il a toutefois clôturé le dossier tout en avertissant le Parlement que, une fois les lignes directrices dans le domaine de la vidéosurveillance adoptées, celui-ci devrait prendre des mesures pour aligner ses pratiques sur les recommandations du CEPD. Ce dernier a aussi fait observer qu'il était possible de continuer à contrôler le respect des règles au travers d'une procédure formelle de contrôle préalable *a posteriori* ou par l'intermédiaire des inspections.

### 2.7.4. Demandes diverses

Sur demande, le CEPD a également donné aux DPD des orientations informelles sur les pratiques de vidéosurveillance. Des questions ont été fréquemment posées concernant la manière dont les personnes concernées devraient être informées et les lieux où il serait approprié et proportionné d'installer des caméras.

Dans un cas, un organe s'est interrogé sur la proportionnalité de l'utilisation d'une caméra cachée afin d'identifier l'auteur de vols répétés de provisions

dans un bureau. Le CEPD a considéré que l'utilisation de caméras cachées était disproportionnée et a recommandé à l'organe de recourir à d'autres méthodes pour détecter ou décourager ce type de comportement.

À la fin de 2008, le CEPD a également été interrogé sur la proportionnalité de l'utilisation de caméras de CCTV dans la salle d'attente d'un service médical. Il examine actuellement le dossier.

## 2.8. Eurodac

Eurodac est une vaste base de données regroupant les empreintes digitales des demandeurs d'asile et des immigrés 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 fonctionnement d'Eurodac et pour recommander des solutions communes. Cette approche de « contrôle coordonné » s'est révélée très efficace jusqu'à présent et a bénéficié de la plus grande attention en 2008 (voir section 4.3).

Au nombre des autres activités menées par le CEPD dans le cadre d'Eurodac figuraient les consultations sur des sujets connexes, notamment des questions relatives à la politique des frontières (voir sections 3.4 et 3.6) et les travaux préparatoires en vue de la révision du règlement Dublin et du règlement Eurodac, sujets sur lesquels le CEPD a rendu des avis en février 2009.

<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).

## 3. Consultation

### 3.1. Introduction

L'année 2008 est la quatrième année complète durant laquelle le Contrôleur européen de la protection des données (CEPD) a pleinement exercé ses fonctions en tant que conseiller des institutions communautaires pour les propositions de législation (et documents connexes). Ce fut une fois encore une année importante au cours de laquelle le CEPD a connu un développement de ses activités. Il a continué de développer et d'améliorer son bilan et a rendu des avis sur un nombre croissant de propositions législatives. En 2008, il a élargi le champ de ses interventions à d'autres domaines d'action de l'Union européenne (UE). De plus, il a étendu sa participation à tous les stades de la procédure législative, depuis le début, notamment en réagissant à un Livre vert sur le patrimoine des débiteurs, jusqu'à la toute dernière phase, en suivant activement les travaux du Parlement européen et du Conseil sur des dossiers importants tels que le système PNR européen et la directive concernant la vie privée et les communications électroniques.

Au travers de sa participation au processus législatif de l'UE, le CEPD a pour objectif 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. L'avis du CEPD est rendu de manière formelle et fait alors partie du processus législatif. Plusieurs avis ont été présentés devant la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, ainsi que devant les groupes concernés du Conseil.

Comme les années précédentes, le CEPD s'est appuyé sur un inventaire des travaux qu'il entendait mener l'année suivante. L'inventaire 2008 a été publié sur le site web du CEPD en décem-

bre 2007. Il comporte une analyse succincte des évolutions les plus importantes et expose les priorités pour 2008.

Le nombre d'avis rendus par le CEPD a constamment augmenté depuis qu'il a commencé à exercer ses fonctions. Quatorze avis ont été rendus en 2008. Ces avis reflètent également les thèmes pertinents figurant dans les programmes de la Commission européenne, du Parlement européen et du Conseil. La majorité des avis concernait des questions liées à l'espace de liberté, de sécurité et de justice, notamment le « troisième pilier » de l'UE (coopération policière et judiciaire), ainsi que la gestion des frontières (dans le cadre du « premier pilier »). Les propositions établies dans ce domaine peuvent, par exemple, promouvoir l'échange d'informations entre les autorités pour lutter contre le terrorisme et d'autres délits, éventuellement à l'aide de bases de données à grande échelle concernant des millions de personnes. L'adoption, en novembre 2008, de la décision cadre 2008/977/JAI 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>(22)</sup> a constitué une étape importante en la matière.

Un certain nombre d'avis ont également porté sur les échanges transfrontaliers d'informations, hors du cadre de la lutte contre le terrorisme, notamment la proposition de directive relative à l'application des droits des patients en matière de soins de santé, de décembre 2008. D'une manière générale, le CEPD a considéré que ces propositions étaient suffisamment motivées pour justifier l'établissement des systèmes en question. Il a toutefois délivré

<sup>(22)</sup> Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350 du 30.12.2008, p. 60).



L'équipe de consultation discute d'un avis dans le domaine législatif.

des recommandations pour que les propositions soient améliorées en ce qui concerne les principaux éléments touchant à la protection des données.

Le CEPD ne s'est pas seulement appuyé sur des avis pour conseiller les institutions de l'UE dans leur travail législatif, il a aussi utilisé d'autres outils pour intervenir, notamment les observations. C'est le cas des observations préliminaires qui ont été formulées par le CEPD au sujet du paquet relatif à la gestion des frontières de l'UE, présenté par la Commission.

Ce chapitre passe en revue les activités menées par le CEPD en 2008 dans son rôle consultatif. Les avis publiés en 2008 sont résumés à la section 3.3.2. Ce chapitre décrit également les conséquences des nouvelles évolutions technologiques pour le CEPD ainsi que les nouveaux développements dans les domaines politique et législatif.

## 3.2. Cadre d'action et priorités

### 3.2.1. Mise en œuvre de la politique de consultation

Le document stratégique intitulé « Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes »<sup>(23)</sup> expose, dans les grandes lignes, la manière dont le CEPD entend remplir sa mission dans le domaine de la consultation. Ce document précise comment le CEPD agit pour remplir sa mission de manière efficace lorsqu'il est consulté sur des propositions de législation.

<sup>(23)</sup> Disponible sur le site web du CEPD ([http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/05-03-18\\_PP\\_EDPSAdvisor\\_FR.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/05-03-18_PP_EDPSAdvisor_FR.pdf)).

Par l'intermédiaire de ce document stratégique, le CEPD entend se définir comme un acteur fiable et solide du processus législatif de l'UE pour les questions relatives au traitement de données à caractère personnel. Adopté en mars 2005, ce document s'est révélé être une base solide pour les activités du CEPD.

Les orientations définies dans ce document s'articulent autour des trois éléments suivants :

- Les questions pour lesquelles le CEPD doit être consulté : le champ d'application est large dans la mesure où, sur de nombreux thèmes, les propositions peuvent avoir une incidence sur la protection des données à caractère personnel.
- La teneur des interventions du CEPD : ces interventions sont fondées sur le postulat général selon lequel il convient de contribuer au processus législatif de manière non seulement critique mais également constructive.
- Le rôle que le CEPD entend jouer dans le cadre institutionnel de l'UE : les institutions considèrent de plus en plus la fonction consultative du CEPD comme allant de soi.

Le document stratégique prévoit différents stades pour les interventions. En règle générale, les services de la Commission européenne associent le CEPD à leurs travaux avant l'adoption formelle d'une proposition par la Commission, le plus souvent parallèlement à la consultation interne qu'elle mène entre ses différents services. À ce stade, le CEPD formule des observations de manière informelle. Après l'adoption de son avis, le CEPD entretient également des contacts informels avec le Conseil, par l'intermédiaire de la présidence et du Secrétariat général. À plusieurs reprises, le CEPD a précisé ses avis concernant la proposition de législation considérée et en a débattu au sein des groupes compétents du Conseil. Des démarches similaires ont été entreprises auprès de la commission LIBE et d'autres commissions du Parlement européen pour l'examen de l'initiative en question. En outre, le CEPD a pris contact de manière informelle avec le Parlement européen – avec les députés ainsi qu'avec les différents secrétariats – tout en étant également disponible pour des discussions plus générales, notamment lors d'auditions publiques. Parmi les éléments nouveaux apparus en 2008, on relèvera la participation active du CEPD aux travaux relatifs à des dossiers législatifs dans les dernières phases de la

procédure législative, en particulier le système PNR européen et la directive concernant la vie privée et les communications électroniques.

En 2009, une attention particulière sera accordée à la manière dont il convient de conseiller la Commission dans les cas où elle n'adopte pas une proposition (adressée au Conseil et/ou au Parlement européen), mais décide par elle-même. Cela vaut pour les cas suivants :

- la Commission adopte des mesures d'exécution (que ce soit dans le cadre de la « comitologie » ou non) ;
- la Commission rend une décision concernant le niveau de protection adéquat dans un pays tiers, conformément à l'article 25, paragraphe 6, de la directive 95/46/CE ;
- la Commission publie une communication.

Dans ces cas précis, un avis formel rendu après que l'adoption par la Commission est intervenue ne peut pas influencer le texte de l'instrument concerné.

Le 28 avril 2008, le CEPD a présenté un autre document stratégique intitulé « Le CEPD et la recherche et le développement technologique dans l'UE ». Le CEPD a décidé de suivre de près le 7<sup>e</sup> programme-cadre pour des actions de recherche et de développement technologique (RDT), lancé par la Commission à la fin de 2006. Il a décidé d'élaborer plusieurs modèles possibles de contribution à des projets de recherche ciblés du programme-cadre. Le but visé à travers ces modèles de contribution est de conseiller la Commission et/ou les promoteurs de projets dans leurs activités pour recourir à des méthodes de RDT respectueuses de la vie privée et de la protection des données et d'encourager la mise au point de techniques et de processus renforçant l'efficacité du cadre juridique de l'UE en matière de protection des données. Le document stratégique énonce les principaux éléments de l'action du CEPD dans ce domaine (voir section 3.6.5).

### 3.2.2. Inventaire 2008

Chaque année, le CEPD publie un inventaire des travaux qu'il entend mener l'année suivante. L'inventaire 2008 a été publié sur le site web du CEPD en décembre 2007.

Cet inventaire fait partie du cycle de travail annuel du CEPD. Une fois par an, le CEPD décrit rétrospectivement son action dans son rapport annuel. De plus, il publie un inventaire des travaux qu'il

entend mener l'année suivante dans le domaine de la consultation. Il fait ainsi rapport sur ses travaux dans ce domaine deux fois par an. Le travail de sélection et de planification nécessaire à l'efficacité de la fonction consultative est un élément important de la méthode de travail du CEPD.

Les sources principales sur lesquelles le CEPD se fonde pour établir son inventaire sont le programme législatif et de travail de la Commission, ainsi que divers documents de planification connexes établis par cette institution. Durant la procédure d'élaboration, plusieurs intervenants de la Commission ont pu apporter leur contribution.

L'inventaire 2008 se compose des éléments suivants :

- une note introductive, qui comprend une brève analyse de la situation ainsi que les priorités du CEPD pour 2008 ;
- une annexe énumérant les propositions pertinentes de la Commission et d'autres documents récemment adoptés ou programmés qui requièrent l'attention du CEPD.

L'annexe relative à 2008, qui a été publiée en décembre 2007, a été actualisée à deux reprises en 2008 (en mai et en octobre).

#### Résultats

L'annexe de l'inventaire 2008 répertoriait 34 documents importants (qualifiés de « rouges ») sur lesquels le CEPD avait l'intention de rendre un avis ou d'entreprendre une démarche analogue. Les résultats obtenus sont les suivants :

Avis rendus	13 documents (dont 3 à la fin décembre 2007)
Observations/autres interventions du CEPD	4 documents
Intervention par l'intermédiaire du groupe de l'article 29	1 document
Propositions de la Commission et/ou avis du CEPD reportés à 2009	14 documents <sup>(1)</sup>
Sans autre intervention du CEPD	2 documents

<sup>(1)</sup> Sept de ces quatorze documents concernent Eurodac et le SIS. Ils ont été regroupés dans l'inventaire 2009.

En outre, la liste énumérait 33 autres dossiers moins prioritaires, qui pourraient éventuellement faire l'objet d'un avis du CEPD ou d'une autre intervention. L'état des travaux à la fin de 2008 offre une image diversifiée.

Attention continue du CEPD (programmes de recherche, questions/matières générales, telles que la santé publique ou les systèmes d'information à grande échelle)	17 documents
Intervention du CEPD en 2008 (observations ou autres actions)	3 documents
Supprimés de la liste sans autre intervention du CEPD	7 documents
Activité de la Commission reportée à 2009	4 documents
Transformé en question « rouge » (avis rendu en 2008)	2 documents

### Priorités pour 2008

**Priorité n° 1 :** En 2008, le CEPD a étudié de près les incidences du traité de Lisbonne et a formulé des observations à ce sujet, même si l'entrée en vigueur du traité dépend notamment des résultats d'un second référendum en Irlande. Ce traité aura des conséquences importantes sur la protection des données.

**Priorité n° 2 :** Le CEPD a continué d'axer son action sur le stockage et l'échange d'informations dans l'espace de liberté, de sécurité et de justice, en mettant notamment l'accent sur la mise en place d'un cadre juridique garantissant la protection des données dans cet espace, compte tenu du champ d'application limité de la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

**Priorité n° 3 :** Le CEPD a continué de suivre de près les développements intervenus dans le domaine de la société de l'information, tels que l'identification par radiofréquence (RFID) et l'intelligence ambiante, et de formuler des observations à leur sujet, dans le prolongement de la communication de la Commission relative à l'identification par radiofréquence, ainsi que des avis qu'il a déjà rendus en la matière. Dans ce contexte, l'accent a largement été mis sur la révision de la directive concernant la vie privée et les communications électroniques.

**Priorité n° 4 :** L'avis rendu par le CEPD sur l'avenir de la directive 95/46/CE a fait l'objet d'un suivi. Le CEPD a pris part à des activités

liées à la mise en œuvre complète de la directive. Il est étroitement associé aux différents débats sur l'avenir de la directive.

**Priorité n° 5 :** Quelques domaines particuliers de l'action de l'UE ont été mis en évidence, notamment la santé publique, les relations entre la protection des données et la collecte et l'utilisation de statistiques, et d'autres activités liées à l'accès du public aux documents.

**Priorité n° 6 :** Nombre d'activités sont centrées sur le transfert de données à des pays tiers, plus particulièrement le transfert des données passager et les évolutions concernant les éventuels principes transatlantiques (essentiellement communs à l'UE et aux États-Unis) sur l'échange d'informations à des fins répressives.

### 3.2.3. Inventaire 2009

#### Priorités du CEPD en 2009

La stratégie du CEPD ne déviara pas des orientations énoncées dans l'inventaire 2008. On peut observer que, en 2008, le respect de la vie privée et la protection des données ont reçu l'attention voulue dans les analyses d'impact mentionnées dans le programme législatif et de travail de la Commission pour 2008.

Les priorités pour 2009 s'inscriront dans le prolongement des priorités de l'année 2008, compte tenu des évolutions intervenues depuis. Les nouvelles propositions mises à part, une attention particulière sera accordée à la communication de la Commission sur le programme de Stockholm pour un espace de liberté, de sécurité et de justice <sup>(24)</sup>. Cette initiative a pour but de définir les priorités et les objectifs de l'évolution future de l'UE dans cet espace et de déterminer les moyens et les initiatives qui permettront de les respecter au mieux. Cette initiative s'étendra à un pacte global sur les migrations, la justice en ligne et un plan d'action sur les drogues. Elle donne au CEPD l'occasion de réfléchir à ses priorités pour les cinq années à venir. Il entend intervenir dans la phase de préparation et rendra un avis après l'adoption. Cela présente aussi l'avantage de coïncider avec le nouveau mandat du CEPD qui commencera en 2009.

<sup>(24)</sup> Communication de la Commission sur le programme de Stockholm pour un espace de liberté, de sécurité et de justice, 2008/JLS/119.

### 3.3. Avis législatifs

#### 3.3.1. Observations d'ordre général

Le CEPD a rendu 14 avis législatifs en 2008. Comme les années précédentes, une partie non négligeable de ces avis porte sur l'espace de liberté, de sécurité et de justice, tant dans le premier pilier que dans le troisième. Ce domaine représente près de la moitié des avis législatifs rendus, soit six avis sur quatorze. La proposition de modification du règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission a également retenu particulièrement l'attention du CEPD. Ce dernier a adopté des avis sur d'autres initiatives importantes dans les domaines suivants : le système d'information du marché intérieur (IMI), les systèmes informatisés de réservation (SIR), la sécurité routière, les statistiques européennes et les soins de santé transfrontaliers.

À partir du récapitulatif des 14 avis, on pourrait conclure que, dans la plupart des cas, le CEPD s'est déclaré favorable aux propositions concernées, tout en demandant qu'elles soient assorties de garanties spécifiques supplémentaires en matière de protection des données.

#### Échange d'informations

La question de l'échange d'informations, qui recouvre en particulier la mise en place de systèmes d'information et l'accès de différentes autorités à ces systèmes à des fins déterminées, a constitué une priorité pour le CEPD. Les échanges d'informations transfrontaliers sont dorénavant utilisés à plus grande échelle.

En 2008, le CEPD a adopté des avis sur des systèmes d'échange d'informations qui ont été proposés dans le cadre du Système d'information du marché intérieur (IMI) et d'Eurojust, dans le domaine de la sécurité routière, dans le domaine de la protection des enfants lors de l'utilisation de l'internet et dans le cadre d'ECRIS, ainsi que du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et de la stratégie européenne en matière d'e-Justice. Le CEPD a analysé les conséquences juridiques liées au développement de différents systèmes informatiques de grande envergure. La conclusion est qu'il convient d'évaluer dûment et soigneusement dans chaque cas la nécessité de ces échanges d'informations. En outre, lorsque ces échanges d'information sont mis en place, ils doivent être assortis de garanties spécifiques en matière de protection des données.

En raison des risques d'utilisation non justifiée, les obligations légales qui conduisent à la création de

bases de données importantes engendrent des risques particuliers pour les personnes concernées. À de multiples reprises, le CEPD a fait part de ses préoccupations quant au manque de garanties entourant l'échange de données à caractère personnel avec les pays tiers. Plusieurs propositions contiennent des dispositions relatives à de tels échanges, et le CEPD a fait remarquer qu'il conviendrait de mettre en place des mécanismes garantissant l'application de normes communes et la prise de décisions coordonnées en ce qui concerne le caractère adéquat du niveau de protection. Les échanges avec les pays tiers ne devraient être autorisés que si ceux-ci garantissent un niveau de protection adéquat des données à caractère personnel ou si les transferts entrent dans le champ d'application de l'une des dérogations prévues par la directive 95/46/CE.

#### Nouvelles technologies

Le CEPD a examiné à plusieurs reprises la question de l'utilisation des nouvelles technologies. Il a demandé maintes fois que les questions de protection des données soient prises en compte le plus tôt possible (« prise en compte du respect de la vie privée dès la conception »). En outre, il a souligné qu'il convenait d'utiliser les outils technologiques non seulement pour assurer l'échange des informations, mais également pour renforcer les droits des personnes concernées. En ce qui concerne ECRIS et la justice en ligne, le CEPD s'est félicité que la personne concernée puisse demander à l'autorité centrale d'un État membre des informations sur ses propres données, pour autant qu'elle soit ou ait été un résident ou un ressortissant de l'État membre requis ou requérant. Dans le domaine de la coordination des systèmes de sécurité sociale, le CEPD a aussi avancé l'idée d'utiliser en tant que « guichet unique » l'autorité la plus proche de la personne concernée. Par conséquent, le CEPD encourage la Commission à favoriser l'utilisation des outils informatiques, en particulier l'accès en ligne, pour que les citoyens puissent avoir un meilleur contrôle des données à caractère personnel les concernant, même lorsqu'ils se déplacent entre différents États membres.

#### Qualité des données

La qualité des données a constitué un thème important. Les données doivent présenter un niveau d'exactitude élevé pour éviter toute ambiguïté concernant le contenu des informations traitées. Il est donc impératif que l'exactitude des données fasse l'objet d'un contrôle régulier et approprié. Par ailleurs, un niveau de qualité élevé des données constitue non seulement une garantie indispensable pour la personne concernée, mais contribue aussi à une utilisation efficace des données par les personnes qui procèdent à leur traitement.

### 3.3.2. Les avis du CEPD

#### Système d'information du marché intérieur (IMI)

Le 22 février 2008, le CEPD a présenté un avis sur la décision de la Commission concernant la mise en œuvre du Système d'information du marché intérieur (IMI) <sup>(25)</sup>. Le Système d'information du marché intérieur (IMI) est un outil informatique qui permet aux autorités compétentes des États membres de s'échanger des informations aux fins de la mise en œuvre de la législation relative au marché intérieur. L'IMI est financé au titre du programme de fourniture interopérable, de services paneuropéens d'administration en ligne aux administrations publiques, aux entreprises et aux citoyens (IDABC)

La principale recommandation du CEPD mentionnait la nécessité d'une base juridique sans faille pour la décision IMI. Pour le CEPD, la base juridique existante (une décision prise au titre du programme IDABC) ne garantissait pas la sécurité juridique nécessaire en raison de doutes sur la nature contraignante de cet instrument. Le CEPD a en outre présenté un certain nombre de propositions concernant les dispositions régissant les aspects de l'IMI qui touchent à la protection des données. Elles ont trait à la transparence et à la proportionnalité, au traitement conjoint et à la répartition des responsabilités, à l'information des personnes concernées, aux droits d'accès, d'opposition et de rectification, à la conservation des données, aux mesures de sécurité et au contrôle conjoint.

#### Éléments de sécurité et éléments biométriques intégrés dans les passeports

Le 26 mars 2008, le CEPD a présenté un avis concernant la proposition de règlement du Parlement européen et du Conseil modifiant le règlement du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, bien qu'il n'ait pas été consulté sur cette proposition <sup>(26)</sup>.

Avec les éléments de sécurité, les données biométriques ont pour objet de renforcer le lien entre le passeport et son titulaire. En vue d'harmoniser les dérogations relatives au passeport biométrique, de nouvelles

mesures ont été introduites dans la proposition : les enfants âgés de moins de six ans sont dispensés de l'obligation de donner des empreintes digitales, de même que les personnes qui en sont physiquement incapables. Par ailleurs, la proposition introduit le principe obligatoire « une personne, un passeport », par mesure de sécurité additionnelle et afin d'offrir une protection supplémentaire pour les enfants.

Le CEPD a recommandé que le règlement proposé soit modifié pour les raisons suivantes :

- l'âge limite pour exempter les enfants doit être défini par une étude cohérente et approfondie ayant pour objet de déterminer la précision des systèmes en conditions réelles et de rendre compte de la diversité des données traitées ; cette étude doit être menée par une institution européenne disposant d'un savoir faire avéré et d'installations appropriées dans ce domaine ;
- introduire une exemption supplémentaire pour les personnes âgées, en fixant un âge limite qui peut reposer sur des expériences similaires (« US Visit » : 79 ans) ; ce type d'exemptions ne doit en aucun cas stigmatiser les personnes concernées ou constituer une discrimination à leur encontre ;
- le principe « une personne, un passeport » ne doit être appliqué qu'aux enfants ayant atteint l'âge minimum fixé ;
- documents « sources » : des mesures supplémentaires doivent être proposées en vue d'harmoniser l'établissement et l'utilisation des documents requis dans les États membres pour la délivrance de passeports (documents « sources ») ;
- mieux harmoniser la mise en œuvre du règlement (CE) n° 2252/2004 : les données biométriques collectées pour les passeports des États membres ne doivent être stockées que sur un support



Le passeport biométrique : un système d'authentification qui requiert des garanties rigoureuses.

<sup>(25)</sup> Avis du 22 février 2008 concernant la décision de la Commission du 12 décembre 2007 relative à la protection des données à caractère personnel dans le cadre de la mise en œuvre du Système d'information du marché intérieur (IMI) (2008/49/CE) (JO C 270 du 25.10.2008, p. 1).

<sup>(26)</sup> Avis du 26 mars 2008 concernant la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres (JO C 200 du 6.8.2008, p. 1).

décentralisé et il faut appliquer des taux d'erreur communs pour les procédures d'enrôlement et de concordance.

### Vie privée et communications électroniques

Le 10 avril 2008, le CEPD a rendu un avis sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») <sup>(27)</sup>.

La proposition vise à renforcer la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques, non pas en transformant entièrement la directive « vie privée et communications électroniques » actuelle, mais plutôt en proposant d'y apporter des modifications appropriées, destinées essentiellement à renforcer les dispositions liées à la sécurité et à améliorer les mécanismes coercitifs.

Cet avis a traité des questions suivantes :

- le champ d'application de la directive « vie privée et communications électroniques », en particulier les services concernés (proposition de modification de l'article 3, paragraphe 1) ;
- la notification des violations de la sécurité (modification proposée créant les paragraphes 3 et 4 de l'article 4) ;
- les dispositions relatives aux témoins de connexion (« cookies »), logiciels espions et dispositifs analogues (proposition de modification de l'article 5, paragraphe 3) ;
- les actions en justice engagées par des fournisseurs de services de communications électroniques et d'autres personnes morales (modification proposée créant, à l'article 13, un paragraphe 6) ; et
- le renforcement des dispositions relatives au contrôle de l'application (modification proposée créant l'article 15 *bis*).

Dans le prolongement de son avis, le CEPD a pris une part très active dans la suite de la procédure législative (voir section 3.6).

<sup>(27)</sup> Avis du 10 avril 2008 sur la proposition de directive modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») (JO C 181 du 18.7.2008, p. 1.)

### Systèmes informatisés de réservation

Le 11 avril 2008, le CEPD a rendu un avis sur la proposition de règlement du Parlement européen et du Conseil instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation <sup>(28)</sup>.

La proposition a pour objectif de mettre à jour des dispositions du code de conduite pour l'utilisation de systèmes informatisés de réservation, qui a été instauré en 1989 par le règlement (CEE) n° 2299/89 du Conseil. Ce code, qui est de moins en moins adapté aux nouvelles conditions du marché, nécessiterait une simplification afin de renforcer la concurrence, tout en maintenant les mesures de sauvegarde fondamentales et en garantissant la fourniture d'informations neutres aux consommateurs.

Les conclusions du CEPD ont été les suivantes :

- Il s'est félicité de l'inclusion dans la proposition de principes sur la protection des données qui précisent les dispositions de la directive 95/46/CE. Ces dispositions renforcent la sécurité juridique et pourraient utilement être assorties de garanties supplémentaires portant sur trois points : l'obtention du consentement pleinement éclairé des personnes concernées pour le traitement de données sensibles ; l'adoption de mesures de sécurité qui tiennent compte des différents services offerts par les SIR et la protection des données dans un contexte de commercialisation.
- En ce qui concerne le champ d'application de la proposition, les critères qui rendent la proposition applicable aux SIR établis dans des pays tiers soulèvent la question de son application pratique, d'une manière qui soit compatible avec l'application de la *lex generalis*, à savoir la directive 95/46/CE.
- Pour une mise en œuvre effective de la proposition, le CEPD a estimé qu'il fallait une vue d'ensemble claire et globale de toute la problématique des SIR qui tienne compte de la complexité du réseau des SIR et des conditions d'accès de tiers aux données à caractère personnel traitées par les SIR.

### Eurojust

Le 25 avril 2008, le CEPD a rendu un avis sur l'initiative prise par un groupe d'États membres en vue de l'adoption d'une décision du Conseil sur le

<sup>(28)</sup> Avis du 11 avril 2008 sur la proposition de règlement instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation (JO C 233 du 11.9.2008, p. 1.)

renforcement d'Eurojust et modifiant la décision 2002/187/JAI <sup>(29)</sup>.

L'initiative vise à renforcer davantage l'efficacité opérationnelle d'Eurojust.

Le CEPD a proposé plusieurs modifications de la proposition, notamment ce qui suit :

- Il conviendrait de faire référence à 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 listes des données à caractère personnel pouvant faire l'objet d'un traitement en vertu de la décision du Conseil devraient rester des listes fermées.
- Il conviendrait d'ajouter une disposition similaire à celle figurant à l'article 38, paragraphe 5 bis, de la proposition de décision du Conseil portant création de l'office européen de police (EUROPOL), afin d'établir que les dispositions du règlement (CE) n° 45/2001 s'appliquent au traitement des données à caractère personnel relatives au personnel d'Eurojust.

### Sécurité routière

Le 8 mai 2008, le CEPD a rendu un avis sur la proposition de directive du Parlement européen et du Conseil facilitant l'application transfrontière de la législation dans le domaine de la sécurité routière <sup>(30)</sup>. L'objectif général de la proposition consiste à réduire le nombre de tués et de blessés ainsi que les dégâts matériels dus aux accidents de la circulation. Dans ce contexte, la proposition vise à établir un système pour faciliter l'exécution transfrontière des sanctions liées à des infractions routières particulières. Afin de contribuer à une application non discriminatoire et plus efficace de la législation à l'encontre des auteurs d'infractions routières, la proposition prévoit la mise en place d'un système d'échange d'informations transfrontière entre les États membres.

Cet avis contenait les recommandations suivantes :

- En ce qui concerne l'information des personnes concernées : la manière dont les personnes concernées seront informées du fait qu'elles ont des droits particuliers dépendra de la forme de la notification de l'infraction. Il est par conséquent

important que la proposition énumère toutes les informations utiles pour la personne concernée dans une langue qu'elle comprend.

- En ce qui concerne les aspects liés à la sécurité : si le CEPD n'a rien à objecter à l'usage d'une infrastructure déjà existante pour l'échange des informations, il insiste sur le fait que cela ne devrait pas entraîner d'interopérabilité avec d'autres bases de données ; il s'est félicité des limites fixées par la proposition aux possibilités d'utilisation des données par les États membres autres que celui où l'infraction a été commise.
- Le CEPD se tient à disposition pour toute autre consultation au sujet des règles communes qui doivent être élaborées par la Commission aux fins des procédures techniques pour l'échange électronique des données entre les États membres, et notamment en ce qui concerne les aspects de ces règles liés à la sécurité.

### Statistiques européennes

Le 20 mai 2008, le CEPD a rendu son avis sur la proposition de règlement relatif aux statistiques européennes <sup>(31)</sup>. La proposition a pour but de réviser l'actuel cadre juridique de base régissant la production de statistiques au niveau européen, en vue de l'adapter à la réalité actuelle et de l'améliorer de manière à pouvoir répondre aux évolutions et défis futurs.

Le CEPD s'est félicité de la proposition, cette initiative devant permettre de disposer d'une base juridique générale solide pour le développement, la production et la diffusion de statistiques au niveau européen. Il a cependant attiré l'attention sur les points suivants :

- il compte bien être consulté sur la législation sectorielle que la Commission pourrait adopter dans le domaine des statistiques afin de mettre en œuvre le règlement à l'étude, une fois que celui-ci aura été adopté,
- le concept de « sujet de données statistiques » devrait être réexaminé afin d'éviter une confusion avec les concepts de protection des données,
- la Commission devrait tenir compte du principe de la qualité des données lors de l'évaluation qualitative,
- le caractère ambigu du concept d'« anonymisation des données » devrait être examiné dans le cadre de la diffusion des données.

<sup>(29)</sup> Avis du 25 avril 2008 sur l'initiative de 14 États membres en vue de l'adoption d'une décision du Conseil sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI (JO C 310 du 5.12.2008, p. 1).

<sup>(30)</sup> Avis du 8 mai 2008 sur la proposition de directive du Parlement européen et du Conseil facilitant l'application transfrontière de la législation dans le domaine de la sécurité routière (JO C 310 du 5.12.2008, p. 9).

<sup>(31)</sup> Avis du 20 mai 2008 sur la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques européennes (COM(2007) 625 final) (JO C 308 du 3.12.2008, p. 1).



Les enfants sont des proies faciles sur Internet. Des mesures appropriées de protection des données sont nécessaires pour les protéger.

### Protection des enfants lors de l'utilisation de l'internet

Le 23 juin 2008, le CEPD a rendu un avis sur la proposition de décision du Parlement européen et du Conseil instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication <sup>(32)</sup>.

Le CEPD a noté avec satisfaction que ce programme est axé sur le développement de nouvelles technologies et l'élaboration d'actions concrètes en vue de protéger plus efficacement les enfants. La protection des données à caractère personnel est une condition essentielle de la sécurité des enfants lorsqu'ils utilisent l'internet. Il faut éviter que les informations personnelles des enfants soient utilisées à mauvais escient, et ce, en suivant les lignes directrices proposées dans le programme, en particulier les suivantes :

- sensibiliser les enfants et les autres parties prenantes telles que les parents et les éducateurs,
- encourager l'élaboration de meilleures pratiques par les entreprises,
- encourager le développement d'instruments technologiques respectueux de la vie privée,
- favoriser l'échange de bonnes pratiques et de connaissances pratiques entre les services

<sup>(32)</sup> Avis du 23 juin 2008 sur la proposition de décision instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'internet et d'autres technologies de communication (JO C 2 du 7.1.2009, p. 2).

concernés, et notamment ceux qui sont chargés de la protection des données.

Il convient de mettre ces actions en œuvre sans oublier que la protection des enfants se fait dans un environnement où les droits d'autres personnes peuvent être en jeu. Le CEPD a en particulier rappelé que la surveillance des réseaux de télécommunications devrait relever de la compétence des services répressifs.

Le CEPD a noté que le programme à l'examen constitue un cadre général dans lequel s'inscriront de nouvelles actions concrètes. Il a recommandé que les services chargés de la protection des données soient étroitement associés à la conception de

ces projets concrets.

### Accès du public aux documents

Le 30 juin 2008, le CEPD a rendu un avis sur la proposition de règlement relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission <sup>(33)</sup>. La proposition a été précédée par une consultation publique. Après l'adoption de la proposition en juin 2008, une audition publique a été organisée par la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen. À cette occasion, les représentants de la Commission européenne ont souligné que la proposition reflétait l'état actuel des réflexions, mais qu'ils étaient disposés à discuter du texte et à examiner des contributions susceptibles de l'améliorer, sans exclure d'autres solutions de rechange.

Voyant dans cette approche ouverte une occasion à saisir, le CEPD a eu pour objectif d'enrichir le débat en soumettant une variante pour l'article 4, paragraphe 5, proposé, une disposition traitant du lien délicat entre l'accès aux documents et les droits relatifs au respect de la vie privée et à la protection des données à caractère personnel. Cette disposition était destinée à donner effet à l'arrêt du Tribunal de première instance dans l'affaire *Bavarian Lager* (affaire T 194/04). Le CEPD a partagé, dans une certaine mesure, les raisons qui ont conduit à rem-

<sup>(33)</sup> Avis du 30 juin 2008 sur la proposition de règlement relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO C 2 du 7.1.2009, p. 7).

placer l'article 4, paragraphe 1, point b), par une nouvelle disposition, mais il n'a pas pu approuver la disposition en tant que telle.

Cette disposition était critiquable pour les motifs suivants :

- Le CEPD n'était pas convaincu que le moment était bien choisi pour apporter une modification, alors qu'un recours était pendant devant la Cour de justice et que des questions fondamentales y étaient en jeu ;
- la proposition ne fournissait pas la solution qui convient car elle comporte une règle à caractère général (la deuxième phrase de l'article 4, paragraphe 5) qui :
  - ne tient pas compte de l'arrêt du Tribunal de première instance dans l'affaire *Bavarian Lager* ;
  - ne satisfait pas à la nécessité d'établir un juste équilibre entre les droits fondamentaux en jeu ;
  - n'est pas viable puisqu'elle renvoie à la législation communautaire sur la protection des données qui n'apporte pas de réponse claire lorsqu'une décision relative à l'accès du public doit être prise ;
- elle contient une règle spécifique (la première phrase de l'article 4, paragraphe 5) qui est bien définie en principe, mais dont la portée est bien trop limitée.

## ECRIS

Le 16 septembre 2008, le CEPD a rendu un avis sur la proposition de décision du Conseil relative à la

création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2008/XX/JAI <sup>(34)</sup>.

La proposition vise à mettre en œuvre l'article 11 de la décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres, en vue de construire et de développer un système informatisé d'échange d'informations entre les États membres. Elle porte création d'ECRIS et définit également les éléments d'un format standardisé pour l'échange électronique d'informations, ainsi que d'autres aspects techniques et généraux de la mise en œuvre visant à organiser et à faciliter les échanges d'informations.

Le CEPD a appuyé la proposition et formulé quelques observations.

- la responsabilité de la Commission à l'égard de l'infrastructure commune du système, ainsi que l'applicabilité du règlement (CE) n° 45/2001, devraient être clarifiées afin de mieux garantir la sécurité juridique.
- La Commission devrait également être responsable du logiciel d'interconnexion d'ECRIS – et non les États membres comme le prévoit la proposition – afin de renforcer l'efficacité de l'échange et de permettre un meilleur contrôle du système.
- Le recours à la traduction automatique devrait bien défini et circonscrit, de façon à favoriser la compréhension mutuelle des infractions sans nuire à la qualité des informations transmises.

## Transparence du patrimoine des débiteurs

En mars 2008, la Commission a publié un Livre vert concernant la transparence du patrimoine des débiteurs <sup>(35)</sup>. Le Livre vert porte sur les mesures susceptibles d'être adoptées au niveau de l'UE afin d'« améliorer la transparence du patrimoine des débiteurs et de renforcer le droit des créanciers d'obtenir des informations, tout en respectant les principes de la protection de la vie privée du débiteur », conformément aux dispositions de la directive 95/46/CE.

Le 22 septembre 2008, le CEPD a rendu un avis sur le Livre vert <sup>(36)</sup> dans lequel il recommandait que les éventuelles actions législatives découlant du Livre

<sup>(34)</sup> Avis du 16 septembre 2008 sur la proposition de décision du Conseil relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2008/XX/JAI (JO C 42 du 20.2.2009, p. 1).

<sup>(35)</sup> COM(2008) 128 final.

<sup>(36)</sup> Avis du 22 septembre 2008 sur le Livre vert de la Commission intitulé « Exécution effective des décisions judiciaires dans l'Union européenne : la transparence du patrimoine des débiteurs » COM(2008) 128 final (JO C 20 du 27.1.2009, p. 1).



Le CEPD contribue à assurer le juste équilibre entre l'accès du public aux documents de l'UE et le respect de la vie privée.

vert prévoient que le traitement des données à caractère personnel effectué par l'ensemble des autorités d'exécution repose clairement sur au moins l'un des fondements juridiques visés à l'article 7 de la directive 95/46/CE. Il a aussi demandé qu'il soit dûment tenu compte du principe de proportionnalité et que toute mesure en matière de transparence du patrimoine des débiteurs respecte le principe de la limitation des finalités et que toute exception s'avérant nécessaire satisfasse aux conditions énoncées à l'article 13 de la directive 95/46/CE.

### Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations

Le 11 novembre 2008, le CEPD a rendu un avis concernant le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel <sup>(37)</sup>. Ce rapport vise à dégager des principes communs pour la protection de la vie privée et des données à caractère personnel, première étape vers l'échange d'informations avec les États Unis aux fins de la lutte contre le terrorisme et les formes graves de criminalité transnationale.

Dans son avis, le CEPD a fait observer que l'impact d'un instrument transatlantique sur la protection des données devrait être soigneusement examiné au regard du cadre juridique existant et de ses conséquences pour les citoyens. Il s'est déclaré favorable à un accord juridiquement contraignant afin d'offrir une sécurité juridique suffisante.

En outre, le CEPD a préconisé davantage de clarté et de dispositions concrètes, en particulier pour ce qui concerne les aspects suivants :

- il convient de réaliser une analyse approfondie de l'adéquation, sur la base des exigences essentielles portant sur les aspects du système relatifs au contenu, à la spécificité et à la surveillance. Le CEPD a estimé que l'instrument général ne pouvait être considéré comme adéquat que s'il était complété par des accords spécifiques appropriés, au cas par cas ;
- un champ d'application bien délimité et une définition claire et commune des finalités répressives poursuivies sont nécessaires ;
- des mécanismes de surveillance solides sont nécessaires, et les personnes concernées doivent disposer de voies de recours, y compris de recours administratifs et juridictionnels ;

- des mesures effectives doivent garantir à toutes les personnes concernées la possibilité d'exercer leurs droits, indépendamment de leur nationalité ;
- il convient de prévoir la participation d'autorités indépendantes compétentes en matière de protection des données, notamment en ce qui concerne la surveillance et l'aide aux personnes concernées.

De plus, le CEPD a recommandé l'établissement d'une feuille de route en vue d'un éventuel accord ultérieur. Il a également préconisé une plus grande transparence dans le processus d'élaboration des principes relatifs à la protection des données. La participation de tous les acteurs concernés, y compris le Parlement européen, est une condition sine qua non pour que l'instrument fasse l'objet d'un débat démocratique profitable et obtienne le soutien et la reconnaissance nécessaires.

### Soins de santé transfrontaliers

Le 2 décembre 2008, le CEPD a rendu un avis concernant la proposition de directive du Parlement européen et du Conseil relative à l'application des droits des patients en matière de soins de santé transfrontaliers <sup>(38)</sup>. La proposition vise à mettre en place un cadre communautaire pour la prestation de soins de santé transfrontières dans l'UE, pour les cas où les soins dont les patients souhaitent bénéficier sont prestés dans un autre État membre que le leur.

Le CEPD soutient les initiatives visant à améliorer les conditions applicables aux soins de santé transfrontières. Il s'est toutefois déclaré préoccupé par le fait que les initiatives communautaires dans le domaine des soins de santé ne sont pas toujours bien coordonnées sur le plan du recours aux TIC, du respect de la vie privée et de la sécurité des données, ce qui empêche l'adoption d'une approche uniforme de la protection des données à l'égard des soins de santé.

Le CEPD s'est félicité de ce que la proposition mentionnait le respect de la vie privée. Il a fait les suggestions suivantes :

- il faudrait inclure une définition des données relatives à la santé qui engloberait toutes les données à caractère personnel présentant un lien clair et étroit avec la description de l'état de santé d'une personne. Elle devrait en principe comprendre les données médicales, ainsi que les données financières et administratives se rapportant à la santé ;

<sup>(37)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11\\_High\\_Level\\_Contact\\_Group\\_FR.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_FR.pdf).

<sup>(38)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-02\\_Cross-border\\_healthcare\\_FR.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-02_Cross-border_healthcare_FR.pdf).

- un article spécifique sur la protection des données devrait donner une vue d'ensemble claire, en décrivant les responsabilités des États membres de l'affiliation et du traitement et en recensant les principaux domaines à développer, à savoir l'harmonisation au niveau des mesures de sécurité et la prise en compte du respect de la vie privée, en particulier dans les applications « santé en ligne » ;
- le modèle communautaire proposé de prescription électronique devrait incorporer le concept de « prise en compte du respect de la vie privée dès la conception » (« privacy by design »).

#### Stratégie européenne en matière de justice en ligne

Le 19 décembre 2008, le CEPD a rendu un avis sur la communication de la Commission intitulée « Vers une stratégie européenne en matière d'e-Justice »<sup>(39)</sup>. Cette communication a pour objet de proposer une stratégie en matière de justice en ligne (e Justice) visant à accroître la confiance des citoyens dans l'espace de justice européen. Le premier objectif d'e-Justice est de renforcer l'efficacité de la justice partout en Europe, au bénéfice des citoyens. L'action de l'UE doit permettre aux citoyens d'accéder à l'information en surmontant les barrières linguistiques, culturelles et juridiques liées à la multiplicité des systèmes.

Le CEPD a appuyé la proposition, compte tenu des observations qu'il a formulées dans son avis et, notamment :

- de prendre en compte la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ;
- d'inclure les procédures administratives dans la justice en ligne ;
- de continuer à privilégier les architectures décentralisées, en confiant des responsabilités claires à tous les acteurs traitant des données à caractère personnel dans le cadre des systèmes envisagés ; la Commission devrait être responsable des infrastructures communes ;
- de veiller à ce que le principe de limitation de la finalité soit dûment pris en compte dans l'interconnexion et l'interopérabilité des systèmes ;
- de veiller à ce que le traitement de données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées respecte les conditions spécifiques prévues par la législation applicable en matière de protection des données.

### 3.4. Observations

Les observations sont un moyen d'intervention plus simple que les avis législatifs. Le CEPD y a recours lorsqu'il juge inutile de procéder à une analyse juridique exhaustive. Les observations comprennent une analyse politique et fournissent des recommandations constructives pour que les mesures envisagées respectent comme il se doit et promeuvent les principes de la protection des données.

#### Gestion des frontières

Le 3 mars 2008, le CEPD a formulé des observations préliminaires sur trois communications de la Commission européenne visant à renforcer la gestion des frontières extérieures de l'UE<sup>(40)</sup>. Les observations portaient essentiellement sur les mesures susceptibles d'inspirer des préoccupations dans le domaine de la protection des données, notamment la création d'un système d'entrée et de sortie prévoyant l'enregistrement d'informations sur les voyageurs, le recours aux données biométriques et la mise en place éventuelle d'une grande banque de données de l'UE afin de stocker ces données.

Le CEPD a souligné que, bien que les mesures envisagées poursuivent un objectif légitime, à savoir rendre les frontières de l'UE plus sûres tout en facilitant les déplacements licites, elles devaient faire l'objet d'un examen attentif, dans la mesure où elles comportaient d'importantes opérations de traitement de données à caractère personnel et présentaient des risques non négligeables de violation de la vie privée. Le CEPD a souligné qu'il était crucial de tenir compte d'une façon appropriée de l'incidence sur les droits au respect de la vie privée des personnes franchissant les frontières de l'UE. Si les garanties en matière de protection des données sont insuffisantes, ces mesures risqueraient non seulement d'avoir des conséquences néfastes pour les personnes concernées, mais elles seraient en outre inopérantes, voire contre-productives, dans la mesure où elles réduiraient la confiance que le public place dans l'action des autorités.

Les observations du CEPD incluaient également des remarques générales concernant l'accumulation des propositions législatives dans le domaine en question, le recours massif aux données biométriques et le manque d'éléments justifiant la création de nouveaux systèmes de données.

<sup>(39)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-19\\_ejustice\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-19_ejustice_EN.pdf).

<sup>(40)</sup> Doc. COM(2008) 69, COM(2008)68 et COM(2008)67.

### **Décision de la Commission sur le système d'information du marché intérieur (IMI) — Suivi de l'avis du CEPD du 22 février 2008**

Le 14 juillet 2008, le CEPD a répondu à une lettre de la Commission proposant une solution pour progresser vers une mise en œuvre plus complète des garanties nécessaires en matière de protection des données, dans le contexte du système d'information du marché intérieur (IMI).

Le CEPD est convenu que l'adoption de lignes de conduite en matière de protection des données, sous la forme d'une recommandation de la Commission, marquait une étape importante et positive dans le sens de la création d'un cadre global de protection des données pour l'IMI. Il a souligné que le champ d'application de l'IMI, actuellement limité à des échanges d'informations dans le cadre des directives relatives aux services et aux qualifications professionnelles, allait progressivement s'élargir vers d'autres domaines de la législation sur le marché intérieur. Cela entraînera une complexité accrue ainsi qu'une augmentation du nombre d'autorités participantes et une intensification des échanges de données. Dans ce contexte, le CEPD croit qu'il sera nécessaire de prévoir, dans des actes législatifs communautaires juridiquement contraignants, des garanties spécifiques en matière de protection des données, allant au-delà de la législation existante dans ce domaine.

### **Service universel, vie privée et communications électroniques — Suivi de l'avis du CEPD du 10 avril 2008**

En ce qui concerne la directive « service universel » et la directive relative à la vie privée et aux communications électroniques, le CEPD a formulé des observations sur certaines questions soulevées dans le rapport de la Commission du marché intérieur et de la protection des consommateurs concernant le réexamen de la directive 2002/22/CE. Le 2 septembre 2008, le CEPD a fait part des préoccupations que lui inspiraient certains amendements *ad hoc* qui figurent dans ledit rapport de la commission et qui, s'ils étaient adoptés, affaibliraient la protection des données à caractère personnel et de la vie privée dont bénéficient les internautes (voir également le point 3.6).

## **3.5. Interventions devant la Cour de justice**

Le CEPD a le droit d'intervenir dans des affaires portées devant la Cour de justice des Communautés européennes en rapport avec ses missions. Ce droit couvre toutes les affaires communautaires relatives au traitement des données à caractère personnel.

Ce droit d'intervention est fondé sur l'article 47 du règlement (CE) n° 45/2001 et concerne également le Tribunal de première instance et le Tribunal de la fonction publique. Lors de ses interventions, le CEPD vise à clarifier les éléments relevant de la protection des données.

Le 1<sup>er</sup> juillet 2008, le CEPD a participé à l'audition dans l'affaire C-301/06, *Irlande contre Conseil et Parlement*. Le CEPD a défendu le point de vue selon lequel l'article 95 du traité CE constituait la base juridique correcte de la directive 2006/24/CE sur la conservation de données <sup>(41)</sup>.

En outre, le CEPD a demandé à intervenir dans les affaires qui suivent :

- affaire C-518/07 (*Commission contre Allemagne*) portée devant la Cour de justice, concernant l'indépendance des autorités chargées de la protection des données ;
- affaire T-3/08 (*Coédo Suárez contre Conseil*) portée devant le Tribunal de première instance, concernant le droit d'accès dans le cadre de la réglementation relative à la protection des données ;
- affaire F-35/08 (*Pachtitis contre Commission*) portée devant le Tribunal de la fonction publique, concernant le droit d'accès dans le cadre de la réglementation relative à la protection des données ;
- affaire F-48/08 (*Ortega Serrano contre Commission*) portée devant le Tribunal de la fonction publique, concernant le droit d'accès dans le cadre de la réglementation relative à la protection des données ;
- affaire T-382/08 (*Advance Magazine Publishers contre OHMI*) portée devant le Tribunal de première instance, concernant l'accès du public aux documents.

Les juridictions concernées ont autorisé le CEPD à intervenir dans les trois premières affaires. Dans l'affaire F-48/08, le recours lui-même a été jugé irrecevable, alors que dans l'affaire T-382/08, le Tribunal ne s'est pas encore prononcé sur la demande du CEPD.

Le CEPD a formulé plusieurs observations sur le fond de trois affaires :

- dans l'affaire C-518/07, le CEPD a présenté un mémoire en intervention pour soutenir la Commission ;
- dans l'affaire C-28/08 P (*Commission contre Bavarian Lager*), le CEPD a répondu au recours formé par la Commission (affaire C-28/08 P)

<sup>(41)</sup> Les plaidoiries peuvent être consultées sur le site web du CEPD.

contre l'arrêt du Tribunal de première instance du 8 novembre 2007 dans l'affaire Bavarian Lager T-194/04 ; le CEPD a également répondu, en tant que partie à la procédure, aux arguments invoqués par les intervenants ;

- dans l'affaire T-374/07 (*Pachtitis contre Commission et EPSO*), le CEPD a présenté un mémoire en intervention au soutien de la Commission.

### 3.6. Autres activités

#### 3.6.1. Vie privée et communications électroniques

La proposition de la Commission en vue de réviser la directive concernant la vie privée et les communications électroniques a requis l'attention permanente du CEPD tout au long de l'année <sup>(42)</sup>.

Le 2 septembre 2008, le CEPD a formulé des observations sur certaines questions concernant le traitement des données relatives au trafic et la protection des droits de propriété intellectuelle <sup>(43)</sup>. Le même mois, le Parlement européen a adopté une résolution législative sur la directive concernant la vie privée et les communications électroniques <sup>(44)</sup>. Parmi les modifications importantes figurait l'inclusion des fournisseurs de services de la société de l'information dans le champ d'application de l'obligation de notifier des violations de la sécurité.

Le CEPD s'est félicité de cette modification ainsi que de l'amendement visant à permettre à toute personne physique ou morale d'intenter une action en cas de violation de toute disposition de la directive concernant la vie privée et les communications électroniques. Le 17 septembre 2008, le CEPD a présenté son point de vue lors d'une audition organisée par des membres de différents groupes politiques du Parlement européen. À d'autres occasions, il a procédé à des échanges de vues avec des membres du Parlement européen et d'autres parties prenantes sur des questions telles que la notification des violations de la sécurité, le traitement des adresses IP et la normalisation en vue de la conception de produits favorisant le respect de la vie privée.

<sup>(42)</sup> Voir aussi le point 3.3.2 concernant les avis ponctuels.

<sup>(43)</sup> Voir le point 3.4.

<sup>(44)</sup> Résolution législative du Parlement européen du 24 septembre 2008 sur la proposition de directive du Parlement européen et du Conseil modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération en matière de protection des consommateurs (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)).



Le CEPD a fourni de nombreux éléments d'information à la Commission européenne, au Parlement et au Conseil concernant le réexamen de la directive « vie privée et communications électroniques ».

En novembre 2008, le Conseil est parvenu à un accord politique sur une révision des règles relatives au paquet télécom, y compris la directive concernant la vie privée et les communications électroniques. Le Conseil a modifié certains éléments essentiels de la proposition et a refusé un grand nombre des amendements adoptés par le Parlement européen. Le CEPD s'est inquiété de la teneur de la position commune, les garanties en faveur des citoyens ayant été supprimées ou sensiblement affaiblies. Le niveau de protection accordé aux personnes dans la position commune s'en trouve considérablement affaibli.

C'est pourquoi le CEPD a annoncé qu'il rendrait un deuxième avis, qui a été adopté le 9 janvier 2009 (et sera examiné dans le rapport annuel pour 2009).

#### 3.6.2. Dossiers passagers

Comme les années précédentes, le CEPD a été étroitement associé aux travaux relatifs aux dossiers passagers (PNR). En 2008, beaucoup d'énergie a été consacrée au suivi de 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>(45)</sup>, c'est-à-dire le régime interne de l'UE pour la collecte et l'exploitation des données des passagers aériens qui entrent dans l'UE ou qui en sortent. Le CEPD a été étroitement associé aux travaux pendant la présidence française et s'est interrogé notamment sur la nécessité et la proportionnalité de ce régime. Les travaux se sont poursuivis sous les présidences tchèque et suédoise.

<sup>(45)</sup> COM(2007)654.

La date d'adoption de la proposition par le Conseil n'est pas connue avec certitude. Le CEPD entend continuer à suivre de près l'évolution des travaux et rendra probablement un deuxième avis.

### 3.6.3. Mise en œuvre du SIS et politique des frontières

Comme indiqué plus haut (point 3.1), le CEPD a une interprétation large de sa mission de conseil sur les propositions législatives. Il s'efforce néanmoins de moduler l'énergie qu'il consacre à sa mission consultative en fonction de l'incidence des propositions sur la protection des données personnelles. Actuellement, les propositions dans le domaine de la liberté, de la sécurité et de la justice revêtent une grande importance. Les questions prépondérantes dans ce domaine sont le partage de l'information dans le cadre de la coopération policière et judiciaire, ainsi que les questions liées aux systèmes d'information à grande échelle, par exemple Eurodac, le Système d'information sur les visas (VIS) et le Système d'information Schengen de deuxième génération (SIS II). Le SIS II consiste en une base de données centrale appelée Système central d'information Schengen (C.SIS), dont la Commission assure la gestion opérationnelle, en liaison avec les points d'accès nationaux désignés par chaque État membre (NI-SIS). Les autorités Sirene assureront l'échange de toute information supplémentaire (liée aux signalements SIS II mais non stockée dans le système lui-même).

Le 30 juin 2008, le CEPD a présenté deux interventions lors d'une table ronde organisée par la Commission LIBE du Parlement européen, associant tant le Parlement européen que des représentants des parlements nationaux. Le thème de cette table ronde était « liberté et sécurité dans le cadre de la gestion intégrée des frontières de l'Union européenne : échange de vues sur le système d'information Schengen de deuxième génération (SIS II), Frontex, Eurosur, le système d'entrée/sortie et le profilage ».

La première intervention du CEPD a porté sur les implications de la migration du SIS I+ au SIS II dans le domaine de la protection des données. Le CEPD a indiqué qu'il comptait organiser un audit concernant l'Unité centrale, qui sera sous sa supervision, au cours des toutes premières phases de fonctionnement, afin de créer un instrument d'évaluation utilisable par la suite. Il a en outre rappelé à quel point la coopération avec les autorités nationales chargées de la protection des données et l'autorité de contrôle commune de Schengen était cruciale pour assurer une transition sans heurt entre les deux systèmes.

Au cours d'une deuxième intervention, à l'occasion d'une session consacrée à la protection de la liberté, de la sécurité et de la vie privée dans le cadre de la future gestion des frontières de l'UE, les observations émises par le CEPD sur le paquet « frontières » ont été mentionnées à plusieurs reprises. Le CEPD a rappelé certains éléments clés, par exemple la nécessité de prendre le temps de la réflexion et d'évaluer la réalité existante avant de lancer de nouvelles propositions. Il a également abordé la question du profilage, qui, malgré son utilité dans certain cas, nécessite des garanties appropriées, compte tenu du risque d'intrusion dans la vie privée des citoyens.

### 3.6.4. Conférence sur la protection des données dans le domaine de la police et de la justice (Trèves)

Les 26 et 27 mai 2008, le CEPD et l'Académie de droit européen (ERA) ont organisé conjointement, à Trèves, une conférence sur l'échange et la protection des données dans le domaine de la liberté, de la sécurité et de la justice. Un aperçu de la législation européenne concernée a été présenté lors du séminaire. L'analyse et la discussion ont porté essentiellement sur les principaux textes relatifs à l'échange de données, par exemple le traité de Prüm ainsi que la décision la plus récente concernant l'intégration du traité au cadre juridique de l'UE. Dans le domaine de la protection des données, le séminaire a porté en particulier sur la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Parmi les autres sujets abordés ont figuré le renforcement du rôle des données recueillies par des sociétés privées à des fins répressives (compagnies aériennes, banques, exploitants de réseaux de télécommunication), les progrès techniques facilitant la collecte des données ainsi que le cadre institutionnel de la protection des données. Enfin, une dernière session a été consacrée à l'avenir, dans la perspective de la mise en œuvre du traité de Lisbonne.

Une centaine de personnes, venues d'un grand nombre d'États membres de l'UE, ont participé à la conférence. Des experts en matière de protection des données et dans le domaine répressif ont examiné le cadre juridique relatif à l'échange et à la protection des données, tel qu'il s'applique actuellement et tel qu'il se présentera dans un proche avenir. De nombreuses interventions ont souligné qu'il importait de conjuguer les considérations relatives à la protection des données et le point de vue des autorités policières et judiciaires, ces deux éléments étant nécessaires à une bonne gouvernance.

### 3.6.5. RDT de l'UE

C'est pendant la phase très précoce au cours de laquelle l'UE déploie des efforts dans le domaine de la recherche et du développement technologiques (RDT) que les principes relatifs à la protection des données et de la vie privée peuvent être efficacement pris en considération, mis en œuvre et promus, conformément au concept de « prise en compte du respect de la vie privée lors de la conception ». En 2008, le CEPD a clarifié et organisé ses contributions possibles à la RDT de l'UE et a consolidé les mesures déjà engagées.



Participation du CEPD à la conférence ICT 2008  
(Lyon, du 25 au 27 novembre 2008).

Parmi les contributions du CEPD à un programme-cadre de recherche et aux appels à propositions, on peut mentionner :

- la participation à des ateliers et à des conférences visant à recenser les défis futurs susceptibles de concerner la politique de l'UE en matière de RDT ;
- la contribution à des groupes consultatifs de recherche créés par la Commission européenne en liaison avec le programme-cadre, ainsi que la présentation d'avis sur les questions relatives à la protection des données ;
- l'aide apportée à la Commission européenne lors de l'évaluation des propositions, notamment en ce qui concerne d'éventuels problèmes qu'elles pourraient poser dans le domaine de la protection des données.

Le CEPD pourrait en outre rendre un avis sur des projets spécifiques en matière de RDT, soit à la demande d'un groupement d'entreprises travaillant sur un projet, soit de sa propre initiative.

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

En avril 2008, le CEPD a adopté un document stratégique intitulé « Le CEPD et la recherche et le développement technologique dans l'UE »<sup>(46)</sup> décrivant le rôle que pourrait jouer l'institution

<sup>(46)</sup> [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28\\_PP\\_RTD\\_FR.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_FR.pdf)

en ce qui concerne les projets de R&D relevant du septième programme-cadre de recherche et développement. Ce document présente les critères de sélection des projets qui peuvent faire l'objet d'une intervention 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.

En novembre 2008, à Lyon, le CEPD a tenu un stand lors d'une manifestation considérée comme la plus grande d'Europe dans le domaine des technologies de l'information et de la communication (TIC). À cette occasion, le document stratégique du CEPD a été présenté à certains des 4500 délégués enregistrés et un appui ciblé leur a été fourni concernant les meilleures manières de traiter les questions relatives à la protection des données qui peuvent se poser dans leurs activités de recherche.

La plupart des nouvelles contributions du CEPD envisagées dans le nouveau document stratégique ont déjà été mises en œuvre en 2008 grâce aux actions ci-après :

- après avoir analysé les différents éléments du projet « Turbine » de l'UE<sup>(47)</sup> (*TrUsted Revocable Biometric IdeNtitiEs*), dont l'objectif est de mener des recherches concernant les données biométriques révocables, le CEPD a décidé de répondre favorablement à la demande

<sup>(47)</sup> <http://www.turbine-project.eu>

- du groupement d'entreprises et rendra un avis sur ce projet en 2010 ;
- en 2008, le CEPD a décidé d'examiner de plus près le projet « Bridge » (Building Radio Frequency IDentification for the Global Environment) <sup>(48)</sup>, en cours d'exécution ; le CEPD a communiqué des recommandations à la Commission européenne après avoir évalué une mission d'information et s'être réuni avec les agents de la Commission chargés du projet ; à la lumière des recommandations formulées par le CEPD, la Commission européenne a pris de nouvelles mesures destinées à clarifier les activités de recherche menées dans le cadre du projet et à les mettre davantage en conformité avec la législation communautaire en matière de protection des données à caractère personnel ;
  - au cours de l'année 2008, le CEPD a fourni à une série de groupements d'entreprises gérant des projets de RDT de l'UE la liste des points de contact des autorités nationales chargées de la protection des données et a facilité l'établissement de contacts ; ces demandes visaient essentiellement à obtenir davantage d'informations sur la législation applicable en matière de protection des données ainsi que des informations de contact plus précises en vue d'éventuelles notifications de traitements de données à caractère personnel.

### Groupes consultatifs de recherche de la Commission européenne

Pour suivre de plus près l'élaboration des nouvelles lignes d'action de l'UE en matière de RDT, le CEPD a accepté de participer en tant qu'observateur aux activités de groupes consultatifs de recherche gérés par la Commission dont la liste figure ci-après, ou d'intervenir au cas par cas dans les activités de ces groupes :

- *Risepitis (Research and innovation for security, privacy and trustworthiness in the information society* – Comité consultatif pour la recherche et l'innovation sur la sécurité, la vie privée et la confiance dans la société de l'information) : en 2008, à l'invitation de la DG Société de l'information et médias de la Commission européenne, le CEPD a accepté de rejoindre ce groupe en tant qu'observateur ; ce groupe consultatif de recherche de haut niveau concernant les TIC ainsi que la sécurité et la confiance vise à fournir des orientations d'avenir relatives aux défis politiques et en matière de recherche dans le domaine de la sécurité et de la confiance dans la société de l'information ;
- *ESRIF (European Security Research and Innovation Forum* – Forum européen de la recherche et de l'innovation en matière de sécurité) : l'ESRIF est un groupe stratégique européen créé en septembre 2007 dans le domaine de la recherche en matière de sécurité civile. Son objectif premier est de concevoir, d'ici 2009, une stratégie à moyen et à long terme pour la recherche et l'innovation en matière de sécurité civile par le biais d'un dialogue entre le public et le privé. Le CEPD est intervenu lors d'une réunion d'un sous-groupe de l'ESRIF chargé des questions relatives à l'innovation ;
- le CEPD est également intervenu, de façon ponctuelle, au sein des groupes consultatifs de la Commission chargés des systèmes informatiques à sécurité multi-niveau ainsi que de la société de l'information omniprésente de l'avenir.

### 3.6.6. Fusion Google / DoubleClick et questions relatives à la protection des données

En mars 2008, la Commission européenne a autorisé, en vertu de la législation de l'UE relative aux fusions, l'acquisition de la société DoubleClick, qui fournit des technologies publicitaires en ligne, par Google, propriétaire de l'un des principaux moteurs de recherche sur internet. Ces sociétés gèrent d'énormes bases de données contenant des données à caractère personnel relatives aux habitudes des internautes en ce qui concerne la recherche et la navigation sur internet. L'exploitation combinée de ces bases de données suscite des questions délicates et complexes liées au droit à la protection des données à caractère personnel.

À la fin janvier 2008, le CEPD a apporté sa contribution à une audition organisée par la Commission LIBE du Parlement européen sur le thème de la protection des données sur internet. En outre, en qualité de conseiller auprès des institutions de la Communauté sur toutes les questions relevant de la protection des données, le CEPD a procédé à un échange de courriers avec Mme Neelie Kroes, membre de la Commission chargée de la concurrence. L'équipe du CEPD a rencontré les agents concernés de la Commission et a mis ses compétences à leur service pour les questions relatives à la protection des données susceptibles de se poser dans des affaires de concurrence telles que cette fusion.

Dans ce contexte, le CEPD se félicite que la Commission ait clairement précisé, dans un communiqué de presse, que sa décision était fondée exclusivement sur la réglementation de l'UE en matière de fusions, sans préjudice des obligations

<sup>(48)</sup> <http://www.bridge-project.eu/>

qui incombent à l'entité fusionnée en vertu de la législation européenne et nationale relative à la protection des données.

En outre, en tant que membre du Groupe article 29 sur la protection des données, le CEPD a activement participé à l'élaboration d'un document sur la protection des données et les moteurs de recherche, adopté par le groupe en avril 2008.

### 3.6.7. Participation à des groupes d'experts

#### Parties prenantes dans le domaine de l'identification par radiofréquences (RFID)

Le groupe d'experts sur l'identification par radiofréquence a été institué par une décision de la Commission du 28 juin 2007<sup>(49)</sup>. Ce groupe est également connu en anglais sous le nom de « RFID – Stakeholders Group » (groupe des parties prenantes sur les RFID). Conformément à l'article 4, paragraphe 4, point b), de la décision, le CEPD participe aux travaux de ce groupe en qualité d'observateur. Au cours des quatre réunions du groupe organisées en 2008, le CEPD a participé à des discussions visant à apporter une contribution à une recommandation qui devrait être diffusée en 2009. Au sein du groupe, le CEPD a en outre contribué à l'analyse de la nature et des effets de l'évolution actuelle menant à la mise en place d'un « internet des objets » ; ces travaux ont débouché sur la publication, en septembre 2008, d'un document de travail des services de la Commission<sup>(50)</sup> et feront l'objet d'une communication qui sera publiée ultérieurement en 2009.

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

La groupe d'experts « plate-forme pour la conservation de données électroniques à des fins de recherche, de détection et de poursuite d'infractions graves » a été institué par la décision de la Commission du 25 mars 2008<sup>(51)</sup>. Il est composé de représentants des services répressifs des États membres, d'organismes actifs dans le secteur des communications électroniques et des autorités chargées de la protection des données, ainsi que de membres du Parlement européen et du CEPD. Ce groupe d'expert joue un rôle de groupe consultatif<sup>(52)</sup>. Il facilitera l'échange des meilleures pratiques et contribuera à l'évaluation que réalisera la Commission concernant les

coûts et l'efficacité de la directive 2006/24/CE (directive sur la conservation de données) ainsi que le développement de technologies susceptibles d'avoir un effet sur la directive<sup>(53)</sup>.

La première réunion officielle du groupe a eu lieu le 28 novembre 2008 (quatre réunions informelles avaient déjà été organisées depuis 2007). Plusieurs documents concernant des aspects techniques et juridiques de la conservation des données sont à l'examen. Le CEPD participe activement aux réunions et continuera d'apporter son soutien en 2009.

#### Historiques de crédit

Le CEPD participe en qualité d'observateur au Groupe d'experts sur les historiques de crédit, dont la première réunion a eu lieu en septembre 2008. Le groupe rassemble des experts issus des registres de crédit, des associations nationales de consommateurs, des banques et des autorités chargées de la protection des données (y compris les autorités françaises et finlandaises de protection des données). En mai 2009, il achèvera un rapport sur la nécessité d'un échange transfrontalier d'informations de crédits concernant les personnes au sein de l'UE ainsi que sur les conditions applicables à un tel échange. Plusieurs aspects du projet suscitent des questions en matière de protection de la vie privée, par exemple la finalité exacte de l'échange d'informations et la qualité des données faisant l'objet du transfert. Le CEPD et les autres autorités représentées dans le domaine de la protection des données ont mis l'accent sur ces questions, l'objectif étant que le rapport du groupe d'experts soit dûment équilibré.

### 3.6.8. Accidents maritimes

En novembre 2008, le CEPD a présenté, en réponse à une demande, un avis ciblé concernant la proposition de directive établissant les principes fondamentaux régissant les enquêtes sur les accidents dans le secteur des transports maritimes. La proposition avait déjà été adoptée par la Commission en 2005 et était parvenue au troisième et dernier stade de la procédure de codécision, à savoir le comité de conciliation. La demande d'avis a été présentée par le rapporteur du Parlement, lui-même membre du comité. Le CEPD a reçu les différents avis du Conseil et du Parlement européen sur un article particulier de la proposition, concernant la collecte de données à caractère personnel et leur éventuelle divulgation. L'avis rendu ensuite par le CEPD a permis au comité de parvenir à un accord

<sup>(49)</sup> Décision n° 467/2007/CE (JO L 176 du 6.7.2007, p. 25).

<sup>(50)</sup> [http://ec.europa.eu/information\\_society/eeurope/i2010/docs/future\\_internet/swp\\_internet\\_things.pdf](http://ec.europa.eu/information_society/eeurope/i2010/docs/future_internet/swp_internet_things.pdf)

<sup>(51)</sup> Décision 2008/324/CE de la Commission (JO L 111 du 23.4.2008).

<sup>(52)</sup> Voir l'article 2 de la décision.

<sup>(53)</sup> Considérant 6 de la décision.

sur la question. Le CEPD a indiqué qu'il se félicitait d'avoir été consulté, pour la première fois à ce stade du processus législatif.

### 3.6.9. Maladies transmissibles

Les maladies transmissibles, par exemple la tuberculose, la rougeole et la grippe, ignorent les frontières nationales et peuvent se propager rapidement. De nouvelles maladies apparaissent, tandis que d'autres développent des formes résistant aux médicaments. En outre, de nouvelles découvertes scientifiques sur le rôle des agents infectieux dans des affections chroniques telles que le cancer, les cardiopathies ou les allergies font actuellement l'objet de recherches. Le réseau de surveillance épidémiologique et de contrôle des maladies transmissibles a été créé en 1999<sup>(54)</sup> pour répondre à toutes ces questions. Ce réseau s'appuie sur les travaux réalisés dans les États membres et comprend deux piliers : la surveillance épidémiologique et un système d'alerte précoce et de réaction. Le CEPD a présenté des observations informelles sur la décision de la Commission modifiant la décision 2000/57/CE concernant le système d'alerte précoce et de réaction pour la prévention et le contrôle des maladies transmissibles.

### 3.6.10. Le Code des douanes communautaire et le numéro d'enregistrement et d'identification des opérateurs économiques (numéro EORI)

La Commission européenne a consulté le CEPD de manière officieuse à propos du projet de modification du règlement (CEE) n° 2454/93 de la Commission du 2 juillet 1993 fixant certaines dispositions d'application du règlement (CEE) n° 2913/92 du Conseil établissant le code des douanes communautaire (ci-après dénommé « le projet »). C'était la première fois que le CEPD était consulté dans la perspective de l'adoption d'un règlement de la Commission, celle-ci étant alors assistée par un comité (le comité du code des douanes en l'occurrence). Le CEPD n'a pas rendu d'avis mais a envoyé à la Commission trois lettres exposant des recommandations.

Le nouvel instrument propose une base juridique pour un système d'identification et d'enregistrement des opérateurs économiques et des autres personnes, prévoyant une procédure d'enregistrement unique pour tous les contacts avec les autorités douanières de l'ensemble de la Communauté. Un système

électronique d'enregistrement et d'identification des opérateurs économiques (EORI) sera créé aux fins du stockage et de l'échange des données concernées entre les autorités douanières et entre celles-ci et la Commission. En outre, les données existantes dans les systèmes nationaux seront centralisées et envoyées périodiquement aux États membres.

Le CEPD a conseillé la Commission sur de nombreux aspects, notamment :

- la fonction de contrôle exercée conjointement par le CEPD et les autorités nationales compétentes en matière de protection des données ;
- la différence entre les « opérateurs économiques » et les « autres personnes » (personnes concernées) eu égard à la nécessité et à la proportionnalité du traitement des données ; l'incidence de ces éléments sur la licéité du traitement, la durée de conservation, etc. ;
- les droits de la personne concernée, le consentement en tant que condition légale de la publication des données à caractère personnel sur internet et l'adoption de mesures de sécurité.

## 3.7. Nouvelles évolutions

### 3.7.1. Interaction avec la technologie

On peut s'attendre à ce que l'évolution des nouvelles technologies, et l'utilisation qui en est faite, contribuent à un changement qualitatif de la société dans son ensemble. Face à ces nouvelles perspectives, on a évoqué la « société de l'information omniprésente », « l'intelligence ambiante » ou « l'internet des objets ». Ces technologies ne seront viables que si les défis qu'elles lancent, surtout en ce qui concerne la protection des données et de la vie privée, sont relevés d'une manière appropriée dès les premières phases de leur mise au point. Une analyse exhaustive des tendances technologiques qui déterminent la transformation de la société européenne en société de l'information est un facteur essentiel pour parvenir à renforcer la confiance placée dans cet environnement émergent, une telle confiance revêtant une importance de premier ordre.

#### Informatique dématérialisée (« cloud computing »)

Dans son rapport annuel pour 2007, le CEPD avait déjà fait part de la vive préoccupation que lui inspire le fait que les questions liées à la protection de la vie privée et à la sécurité n'étaient pas encore résolues alors que se développe l'informatique dématéri-

<sup>(54)</sup> Décision 2119/98/CE du Parlement européen et du Conseil.



L'informatique dématérialisée intègre des silos de données et remet en question la mise en œuvre du cadre réglementaire de l'UE en matière de protection des données.

sée <sup>(55)</sup>. Les garanties appropriées, nécessaires pour permettre à cette technologie émergente de se développer de manière viable, ne sont pas encore en place. Parallèlement, de plus en plus de services exploitant des systèmes relevant de l'informatique dématérialisée sont proposés non seulement aux entreprises et aux services publics mais aussi aux particuliers.

Le principe de l'informatique dématérialisée représente un véritable défi pour l'identification de la législation applicable au traitement des données à caractère personnel, des responsables et des autres conséquences juridiques en la matière. Les exemples qui suivent témoignent de la souplesse que peut offrir l'informatique dématérialisée mais aussi des questions qu'elle suscite pour l'application du cadre

<sup>(55)</sup> L'informatique dématérialisée (« cloud computing ») désigne le recours aux technologies informatiques sur internet (« nuage ») pour toute une gamme de services. Il s'agit d'un mode d'utilisation des technologies informatiques dans lequel des ressources pouvant être modulées de manière dynamique et souvent virtualisées sont fournies à titre de service sur internet. Du point de vue des utilisateurs, aucune connaissance, compétence ou maîtrise n'est nécessaire en ce qui concerne l'infrastructure qui forme le support de ces technologies et qui se trouve dans le « nuage ».

juridique de l'UE. Pour réduire le coût énergétique, les activités exploitant l'informatique dématérialisée pourraient avoir lieu principalement dans des centres de données fonctionnant à l'énergie solaire et exposés au soleil au moment de la demande de traitement ; au contraire, les centres se trouvant momentanément sur la face non exposée de la terre ou recourant à d'autres sources d'énergie pourraient être moins utilisés. Si cet exemple est attrayant d'un point de vue environnemental, il montre également qu'il serait pratiquement impossible de déterminer à quel endroit le traitement sera effectué et par quel intervenant dématérialisée informatique. Il pourrait en outre arriver que la communication de données à caractère personnel stockées dans des centres se trouvant dans des pays tiers soit demandée, et que ces données soient divulguées aux autorités de la juridiction où se trouvent les serveurs faisant partie du nuage.

Une des solutions possibles déjà proposée serait d'imposer que les données à caractère personnel soient stockées et traitées exclusivement dans des serveurs faisant partie d'un « nuage de l'UE », c'est-à-dire physiquement situés sur le territoire de l'UE et soumis au

cadre réglementaire de l'UE en matière de protection des données. Cette contrainte irait toutefois à l'encontre des fondements d'une technologie prometteuse ainsi que de la souplesse et de l'adaptabilité importantes que l'informatique dématérialisée est censée offrir. Cette proposition semble également négliger le fait que le cadre de l'UE en matière de protection des données s'applique *actuellement* indépendamment du lieu où les données sont traitées, pour autant que le traitement soit effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'UE ou que les moyens utilisés soit situés sur le territoire de l'UE (voir l'article 4 de la directive 95/46/CE). Il n'en reste pas moins que les incertitudes qui planent encore sur l'informatique dématérialisée sont autant de nouveaux défis pour l'application effective et la force exécutoire des normes en matière de protection des données.

Bien entendu, on pourrait envisager de chiffrer les données avant de les transmettre dématérialisée mais, de nouveau, cette procédure ne permettrait pas de tirer parti de la puissance de traitement qu'offre l'informatique dématérialisée, puisque ces données ne pourraient être traitées dès qu'elles auraient été chiffrées <sup>(56)</sup>. Toutefois, pour susciter la confiance dans ces nouveaux environnements, il importera de renforcer la sensibilisation des principaux intervenants au sujet des risques existants et des responsabilités qui incombent à chacun pour y faire face d'une manière adéquate et efficace.

### Séquençage de l'ADN

Grâce aux efforts considérables de R&D déployés dans le cadre du Projet génome humain <sup>(57)</sup>, les gènes humains ont pu être presque complètement séquencés en 2001. Environ trois milliards de paires de bases et entre 20 et 25 000 gènes ont été localisés et identifiés.

Il faudra encore environ deux ans pour que le « Archon X Prize for Genomics » <sup>(58)</sup> puisse être emporté. Toutefois, de nombreuses entités privées sont apparues dans le domaine du test génétique et proposent déjà, pour moins de 400 euros, des analyses portant sur l'identification de traits spécifiques et d'éventuelles maladies.

<sup>(56)</sup> Voir à ce sujet l'article de M. Carl Hewitts, professeur émérite au Massachusetts Institute of Technology (<http://carlhewitt.info/>).

<sup>(57)</sup> [http://www.ornl.gov/sci/techresources/Human\\_Genome/home.shtml](http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml)

<sup>(58)</sup> Ce prix sera accordé à la première équipe qui parviendra à construire un appareil lui permettant de séquencer 100 génomes humains en 10 jours au plus pour un coût ne dépassant pas 10 000 dollars US par génome (<http://genomics.xprize.org/>).

Ce secteur, qui connaît une croissance spectaculaire, est soutenu principalement par les tendances technologiques suivantes :

- les énormes capacités de traitement nécessaires pour l'analyse de quantités colossales de données sont de plus en plus largement disponibles grâce au développement de centres de données interconnectés ;
- l'essaimage d'entreprises et les percées dans le domaine de l'analyse de l'ADN générés par le Projet génome humain ;
- les autres tendances technologiques déjà décrites dans des rapports annuels antérieurs du CEPD, c'est-à-dire la bande passante et la capacité de stockage illimitées.

Les services d'analyse génétique offerts par ces sociétés reposent sur l'exactitude scientifique des liens qu'elles établissent entre les informations génétiques relatives à la personne concernée et les traits ou maladies qui y sont éventuellement liés. De tels liens de causalité sont établis sur la base de nombreux éléments, par exemple l'analyse statistique ou les rapports de R&D disponibles, c'est-à-dire, en résumé, grâce à la capacité de ces sociétés à accéder à de grandes bases de données scientifiques fiables.

Comme l'a récemment relevé une décision de la Cour européenne des droits de l'homme dans une affaire concernant le recours à l'ADN à des fins répressives <sup>(59)</sup>, des échantillons génétiques peuvent révéler de nombreuses informations sensibles sur une personne, y compris sur sa santé et, dès lors, le traitement de ces échantillons doit être soumis aux garanties les plus strictes en matière de protection de la vie privée et des données à caractère personnel.

Des analyses génétiques sont de plus en plus souvent proposées par internet et, par conséquent, à toute personne résidant à l'intérieur ou à l'extérieur du pays où se trouve la société. Ces tests, qui n'étaient auparavant disponibles que dans les secteurs médicaux et judiciaires, strictement réglementés, sont dorénavant offerts commercialement. L'échantillon d'ADN analysé n'appartient pas nécessairement à la personne qui l'envoie mais pourrait être soumis par un tiers ayant pu le recueillir.

À défaut d'une gestion appropriée, la technologie prometteuse permettant un séquençage ultrarapide de l'ADN et la disponibilité de cette technologie au niveau international compromettent les garanties traditionnelles limitant l'accès aux données à caractère personnel les plus sensibles et soulèveront des questions d'importance critique en matière de protection de la vie privée.

<sup>(59)</sup> Affaire S. et Marper contre Royaume-Uni, 5 décembre 2008.

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

#### Le traité de Lisbonne

En 2008, une réflexion sur les conséquences de l'entrée en vigueur du traité de Lisbonne a été engagée. Dans cette perspective, le CEPD a fait le point sur les effets du nouveau traité dans le domaine de la protection des données, par exemple eu égard à la nouvelle base juridique en la matière, à savoir l'article 16 du traité sur le fonctionnement de l'Union européenne, ainsi qu'à l'abolition de la structure en piliers. Le traité ayant été rejeté par l'Irlande le 12 juin 2008, ces activités n'ont pas été poursuivies. Il semblerait maintenant que le traité de Lisbonne puisse entrer en vigueur à la fin de l'année 2009 ou au début de l'année 2010.

#### Programme de travail et programme législatif de la Commission pour 2009, programme de Stockholm

Le programme législatif et de travail de la Commission pour 2009, suivant une approche ciblée, porte essentiellement sur un petit nombre de nouvelles initiatives politiques. Dans le cadre de cette approche, l'accent a été mis résolument sur la réalisation d'analyses d'impact avant que la Commission présente une proposition, ainsi que sur l'évaluation de la législation européenne en vigueur ainsi que des propositions en cours d'examen.

La Commission compte se conformer à la même ligne de conduite dans le domaine de la liberté, de la sécurité et de la justice. Le programme législatif et de travail de la Commission pour 2009 mentionne l'achèvement du programme de La Haye pour la liberté, la sécurité et la justice (novembre 2004) ainsi que de nouvelles mesures en vue de l'instauration d'une politique commune en matière de migrations. Le nouveau programme pluriannuel dans le domaine de la liberté, de la sécurité et de la justice (souvent appelé « programme de Stockholm »), qui doit être adopté pendant la présidence suédoise du Conseil, constitue une nouvelle avancée essentielle figurant au programme de la Commission. Le groupe consultatif de haut niveau sur l'avenir de la politique intérieure européenne (ou groupe sur l'avenir de la politique intérieure) a placé l'équilibre entre mobilité, sécurité et vie privée au cœur de son rapport. Ce rapport, ainsi que le principe de convergence qui y est introduit, figureront parmi les composantes essentielles du programme de Stockholm.

#### Principales tendances dans le domaine répressif

L'inventaire pour 2007 relevait que les activités législatives dans le domaine de la lutte contre la criminalité, notamment le terrorisme et la criminalité organisée, constituaient une des principales tendances de l'année en question. Cette tendance s'est maintenue en 2008.

Par ailleurs, de nouveaux instruments législatifs ont été proposés en complément d'instruments existants qui ne sont pas encore pleinement mis en œuvre. La question s'est posée de savoir si ces nouveaux instruments étaient nécessaires et s'il ne valait pas mieux mettre l'accent sur l'application concrète des instruments existants. Le CEPD abordera ce point dans ses nouvelles contributions aux discussions consacrées à la proposition relative aux dossiers passagers dans l'UE.

Enfin, la tendance à l'ouverture des bases de données existantes (européennes et nationales) vers le domaine répressif se poursuivra en 2009, même si leur finalité était initialement autre. À ces questions sont liées la problématique de l'interopérabilité et de l'interconnexion des bases de données, ainsi que les activités de profilage des personnes.

#### Décision-cadre relative à la protection des données

Dans le domaine législatif, grâce à l'adoption de la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, un cadre juridique général concernant la protection des données dans ce domaine a été établi pour la première fois à l'échelle de l'UE. Néanmoins, la décision-cadre ne s'appliquant pas à tous les cas concernés, d'autres instruments relatifs à la protection des données dans ce domaine restent en vigueur.

Tout au long des négociations, le CEPD a accordé une attention particulière à cet acte législatif, qui a fait l'objet de trois avis ainsi que d'observations. Dans ses avis, le CEPD a reconnu que cette initiative constituait une avancée notable en ce qui concerne la protection des données dans le domaine de la coopération policière et judiciaire en matière pénale, ainsi que le complément indispensable d'autres mesures prises afin de faciliter l'échange transfrontalier de données à caractère personnel en matière répressive. Parallèlement, le CEPD a préconisé à plusieurs reprises d'apporter des améliorations substantielles à la proposition, afin de garantir le respect de normes exigeantes pour ce qui est du niveau de protection offert, tout en mettant en garde contre une dilution

des normes appliquées à la protection des données. Il a notamment regretté le fait que la décision-cadre ne couvre que les données policières et judiciaires échangées entre États membres, autorités et systèmes de l'UE, et non les données internes.

D'autres mesures seront dès lors nécessaires, que ce soit en vertu du traité de Lisbonne ou non, pour renforcer le niveau de protection prévu par le nouvel instrument. C'est pourquoi le CEPD encourage les institutions communautaires à entamer dès que possible la réflexion sur de nouvelles améliorations du cadre de la protection des données en matière répressive.

#### **Avenir de la directive concernant la protection des données**

Des discussions ont eu lieu à différents niveaux sur l'avenir de la directive 95/46/CE. Ces discussions ont porté essentiellement sur l'application de la directive, sans exclure la possibilité de la modifier à l'avenir. L'examen en cours peut être l'occasion de réfléchir à la nécessité de modifier la directive pour veiller à ce qu'elle reste efficace ou d'adopter des règles spécifiques pour résoudre les problèmes relatifs à la protection des données que posent les nouvelles technologies de l'information et de la communication.

De nombreuses activités ont déjà été engagées et s'achèveront dans le courant de 2009. Outre les travaux menés par le Groupe Article 29, on peut mentionner les activités suivantes :

- La Commission a annoncé la tenue d'une consultation publique sur la directive, notamment lors d'une conférence réunissant l'ensemble des intervenants, organisée en mai 2009.
- L'an dernier, le bureau du commissaire à la protection des données du Royaume-Uni (ICO) a lancé un appel d'offres en vue d'évaluer les forces et les faiblesses de la législation de l'UE en matière de protection des données et de recommander des adaptations permettant d'alléger la charge administrative qu'elle occasionne. L'étude examinera la directive de l'UE sur la protection des données ainsi que son application, afin de recenser de meilleures façons de protéger efficacement les particuliers et la société tout en réduisant les charges qui pèsent sur les organisations. L'étude fera l'objet d'une discussion lors de la conférence annuelle de printemps des commissaires européens chargés de la protection des données, en avril 2009, et sera publiée en mai 2009. Quoique seule la Commission européenne puisse engager le processus de modification de la directive, le

bureau du commissaire à la protection des données du Royaume-Uni souhaite lancer un débat sur les forces et les faiblesses de cet instrument afin de garantir que la législation de l'UE en matière de protection des données réponde bien aux besoins des organisations et des particuliers.

#### **Santé publique**

L'UE, estimant qu'il existe de grandes possibilités d'amélioration de la santé des citoyens au niveau transfrontalier par le recours aux technologies de l'information, dispose d'un programme ambitieux en la matière. La santé publique est un nouveau domaine réclamant l'attention du CEPD. L'accent sera mis sur les systèmes d'information dans le domaine de la santé, le développement de systèmes de santé en ligne, l'exploitation secondaire des données médicales, la question de la gestion des activités législatives couvrant des informations sensibles ainsi que d'autres problématiques fondamentales, tout en tenant compte des critiques formulées dans le monde médical à l'égard de la législation sur la protection des données.

Il va sans dire que l'amélioration de la santé au niveau transfrontalier et le recours à cette fin aux nouvelles technologies de l'information ont d'importantes implications pour la protection des données à caractère personnel. L'amélioration de l'efficacité des échanges d'informations dans le domaine de la santé et, partant, l'intensification de ces échanges, l'accroissement de la distance entre les personnes et les instances concernées, le fait que les règles en matière de protection des données soient mises en œuvre par différentes législations nationales sont autant d'éléments qui suscitent des questions concernant la sécurité des données et la sécurité juridique. Le principe de la traçabilité jouera un rôle important.

#### **Divers**

En 2009, le CEPD mettra l'accent sur certains domaines d'action de l'UE :

- la relation entre la protection des données et la collecte et l'exploitation de statistiques ;
- les activités concernant l'accès du public aux documents, par exemple la modification du règlement (CE) n° 1049/2001 sur l'accès du public aux documents.

Enfin, une attention particulière sera accordée en 2009 à la manière dont il convient de conseiller la Commission dans les cas où elle n'adopte pas une proposition (adressée au Conseil et/ou au Parlement européen), mais décide par elle-même.

## 4. Coopération

### 4.1. Le 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>(60)</sup>. Sa mission, décrite à l'article 30 de la directive, peut être résumée comme suit :

- donner à la Commission européenne, au nom des États membres, un avis autorisé 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

<sup>(60)</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 les organismes communautaires (c'est-à-dire le CEPD) et d'un représentant de la Commission. Cette dernière assure également le secrétariat du groupe. Les autorités nationales de contrôle de l'Islande, de la Norvège et du Liechtenstein (partenaires EEE) sont représentées en tant qu'observatrices.

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 devrait jouer un rôle central dans la mise en œuvre homogène de la directive et l'interprétation de ses principes généraux.

En février 2008, le groupe a adopté un nouveau programme de travail bisannuel <sup>(61)</sup>. Il a décidé de se concentrer sur quatre thèmes stratégiques principaux et quelques questions ponctuelles qu'il a jugés le plus pertinents et le plus urgents en vue du renforcement de la protection des données.

Le groupe a recensé trois grands défis :

- les modalités du renforcement des effets de la directive 95/46/CE et du rôle du groupe ;
- l'incidence des nouvelles technologies ;
- l'environnement mondial (les transferts de données au niveau international, la protection de la vie privée à l'échelle planétaire, le problème de la juridiction).

Les quatre thèmes stratégiques exposés plus en détail dans le programme de travail sont les suivants :

- améliorer la mise en œuvre de la directive 95/46/CE ;
- garantir la protection des données lors des transferts internationaux ;
- garantir la protection des données compte tenu du développement des nouvelles technologies ;
- renforcer l'efficacité du Groupe Article 29.

<sup>(61)</sup> Programme de travail pour 2008-2009, adopté le 18 février 2008 (WP 146).

En application de ce programme de travail, le groupe a déjà accompli des progrès notables dans plusieurs domaines :

- transferts internationaux : une série de documents de travail destinés à faciliter le recours à des règles d'entreprise contraignantes (WP 153-155) et le suivi constant des questions relatives aux dossiers passagers (WP 151) ;
- nouvelles technologies : avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche (WP 148) et avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») (WP 150) ;
- amélioration de l'efficacité du groupe : mandat pour une deuxième enquête commune sur le respect, au niveau national, des exigences en matière de protection des données dans le cadre de la conservation des données relatives au trafic (WP 152) ;
- amélioration de la mise en œuvre de la directive 95/46/CE : travaux en cours sur les notions de « responsable du traitement » et de « sous-traitant » ainsi que sur la question de la législation applicable.

Le groupe a en outre suivi de près l'évolution de la situation en ce qui concerne la gestion, la sécurité et le contrôle des frontières de l'UE (système électronique d'autorisation de voyage pour les États-Unis), les données biométriques et les demandes de visas.

Dans ce contexte, le groupe a également pris position sur des propositions législatives ou des documents similaires. Dans certains cas, ces questions avaient 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 contributions du groupe sont aussi très utiles, en particulier parce qu'elles peuvent attirer l'attention sur des points particuliers présentant de l'intérêt sur le plan national. Par conséquent, le CEPD salue ces contributions qui sont allées dans le même sens que ses propres avis.

D'une façon plus générale, le CEPD et le groupe de travail ont coopéré de manière étroite et en bonne synergie sur plusieurs questions, l'accent étant mis surtout sur la mise en œuvre de la directive 95/46/CE et sur les défis que constituent les nouvelles technologies. Le CEPD a par ailleurs résolument

soutenu les initiatives prises afin de faciliter les flux internationaux de données (par exemple les règles d'entreprise contraignantes).

Conformément à l'article 46, point f), i), du règlement (CE) n° 45/2001, le CEPD doit également coopérer avec les autorités nationales de supervision dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toute information utile et en demandant ou en fournissant toute aide nécessaire à l'exécution de leurs tâches respectives. Cette coopération se met en place au cas par cas.

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 supervision (voir le point 4.3).

## 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 bon moyen d'assurer une approche plus 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. Deux réunions ont dès lors été organisées au cours du premier semestre de 2007. La présidence portugaise avait prévu une réunion supplémentaire, qui a été annulée.

La présidence slovène a convoqué une seule réunion du groupe en mai 2008. Au cours de cette réunion, le Contrôleur adjoint a présenté l'avis du CEPD sur l'examen de la directive concernant la vie privée et les communications électroniques, le rapport annuel du CEPD pour 2007 ainsi que les priorités du CEPD en ce qui concerne la consultation relative aux propositions de nouveaux instruments législatifs en 2008.

Un échange de vues a en outre été consacré à la directive 95/46/CE, sur la base notamment de certaines questions telles que le rapport entre la protection des données au titre de la directive et les libertés d'information et d'expression, la nécessité

de dispositions spécifiques eu égard à l'évolution technologique (nouvelles technologies à risque) et la simplification des exigences en matière de notification et d'information (surtout pour les PME).

À l'issue de cet échange de vues, il est apparu que la directive 95/46/CE suscitait la satisfaction générale. Toutefois, une nouvelle discussion d'ensemble sera nécessaire après l'éventuelle ratification du traité de Lisbonne.

Le groupe ne s'est pas réuni pendant la présidence française mais la présidence tchèque a prévu une nouvelle réunion en mars 2009.

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

### 4.3. Supervision coordonnée d'Eurodac

La coopération avec les autorités nationales chargées de la protection des données, en vue d'instaurer une approche coordonnée pour la supervision d'Eurodac (voir le point 2.8), s'est renforcée 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 deux fois en 2008, en juin et en décembre. Cette année, l'accent a été mis sur la mise en œuvre du programme de travail adopté par le groupe en décembre 2007.

Parallèlement, l'attention s'est portée sur le cadre dans lequel le groupe intervient : la Commission européenne a entrepris le réexamen des règlements Dublin et Eurodac dans le contexte des mesures d'asile en général <sup>(62)</sup>.

Désireuse de recueillir des informations communiquées par plusieurs intervenants, la Commission LIBE du Parlement européen a organisé le 29 mai 2008 une table ronde sur le thème « Le »système« de Dublin : où sont les failles, quelles sont les alternatives ? » Le CEPD a eu l'occasion de présenter certains points de vue sur la question et a notamment mis

<sup>(62)</sup> Le 3 décembre 2008, la Commission européenne a présenté plusieurs propositions en vue de « renforcer les droits des demandeurs d'asile en Europe ». Ce train de mesures comporte trois propositions visant à examiner les conditions d'accueil des réfugiés dans l'UE, le règlement Dublin II et le règlement Eurodac, au titre duquel la base de données Eurodac a été créée.

l'accent *sur la façon* dont la supervision coordonnée d'Eurodac pourrait contribuer à l'amélioration du système.

Le groupe est conscient de ces évolutions et prêt à concourir à l'élaboration de nouveaux instruments en partageant et en évaluant les expériences acquises au niveau national.

#### Activités du groupe en 2008

Lors de la réunion de juin 2008, comme prévu à l'article 3 de son règlement intérieur, le groupe a élu un président et un vice-président. Deux candidats se sont présentés : M. Peter Hustinx (CEPD) à la présidence et Mme Guro Slettemark (autorité norvégienne de la protection des données) à la vice-présidence. Les deux candidats ont été élus à l'unanimité des votes valables.

Lors de la réunion de décembre 2007, le groupe avait sélectionné, dans le programme de travail, trois questions devant faire l'objet d'un examen plus étroit et d'un rapport. Le groupe a mis l'accent sur ces trois thématiques en 2008, le travail se déroulant d'abord au niveau national, à l'aide de questionnaires types. L'objectif était ensuite de compiler et d'analyser les réponses pour proposer des conseils lorsque c'est approprié et utile.

#### • Information des personnes concernées

Selon le rapport de l'inspection coordonnée de 2007, si les personnes concernées ont peu exercé le droit d'accès dont elles bénéficient, c'est probablement parce qu'elles connaissent mal ce droit. Le groupe a décidé d'examiner la façon dont les informations sont fournies aux demandeurs d'asile et aux autres personnes qui, pour toute autre raison, font l'objet d'un signalement dans Eurodac. L'objet de cet exercice est de répertorier et d'échanger les meilleures pratiques en la matière (quelles sont les langues utilisées ?, l'incidence des informations est-elle mesurée d'une façon ou d'une autre ?, et autres questions du même ordre).

#### • Enfants et Eurodac

Selon l'article 4 du règlement Eurodac, les empreintes digitales des demandeurs d'asile âgés de 14 ans au moins doivent être relevées. Or, il est souvent difficile d'établir l'âge d'un enfant dépourvu de document d'identité fiable. Le groupe examinera la question des règles fixées et des méthodes utilisées par l'autorité nationale Eurodac pour déterminer si

le demandeur est mineur, et évaluera la conformité de ces règles avec la convention des Nations unies relative aux droits de l'enfant.

Des inspections nationales ont été lancées en août 2008 dans ces deux domaines. Le rapport concernant ces deux inspections est attendu pour la mi-2009.

- **DubliNet** <sup>(63)</sup>

Comme troisième sujet à aborder lors d'une inspection coordonnée, le groupe a choisi l'utilisation de DubliNet et en particulier les questions qui se posent à cet égard en matière de sécurité des données. Le groupe se penchera sur les questions qui suivent : Quelles sont les règles régissant l'échange de données par DubliNet au niveau national ? Quelles sont les mesures prises pour assurer la protection des données à caractère personnel lors d'un tel échange d'informations ? Comment les autres utilisations sont-elles réglementées ?

Pour toutes ces questions, les travaux du groupe tombent à point nommé, compte tenu de la révision des règlements Eurodac et Dublin. Les rapports produits par le groupe devraient contribuer utilement au réexamen de ces textes.

Enfin, le règlement intérieur du groupe a été révisé en décembre 2008 en raison de l'adoption par le CEPD de nouvelles modalités de remboursement des frais de déplacement, qui peuvent également couvrir les indemnités journalières. Le règlement intérieur du groupe a dû être modifié en conséquence.

#### 4.4. Troisième pilier

La nécessité d'une coopération étroite entre le CEPD et les autres autorités chargées de la protection des données dans le domaine de la coopération policière et judiciaire revêt une importance croissante depuis ces dernières années, en raison des nombreuses initiatives prises au niveau de l'UE ou au niveau international en vue de collecter et de partager des données à caractère personnel, initiatives passant parfois par la création et l'interconnexion de bases de données.

Tout d'abord, 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 » (article 46, point f, ii), du règlement (CE) n° 45/2001). Ces organes de contrôle sont les autorités de contrôle communes (ACC) de Schengen, d'Euro-pol, d'Eurojust et du système d'information douanier (SID). La plupart de ces organes sont composés de représentants des autorités nationales de contrôle, qui sont en partie les mêmes, et sont soutenus par un secrétariat commun à la protection des données, au sein du Conseil de l'Union européenne.

En outre, le CEPD coopère avec les autorités nationales chargées de la protection des données, en particulier en participant au groupe de travail « Police et Justice », qui a été chargé par la conférence européenne de surveiller l'évolution de la situation en matière répressive, pour ce qui concerne le traitement des données à caractère personnel, afin de préparer toutes les mesures nécessaires devant être prises par la conférence à cet égard, et d'agir pour le compte de la conférence lorsqu'une réaction rapide est nécessaire de toute urgence.

Le CEPD a participé activement aux réunions du groupe organisées en 2008. Dans nombre de cas, le CEPD a contribué à la discussion en présentant ses avis ou en participant à des sous-groupes. Le CEPD a également été invité à présenter les changements que le traité de Lisbonne entraînerait, surtout dans le domaine de la coopération policière et judiciaire. Le groupe a examiné plusieurs questions délicates, notamment :

- en ce qui concerne la mise en œuvre du traité de Prüm dans l'ordre juridique de l'UE, le groupe a envoyé une lettre au président de la Commission LIBE du Parlement européen et a adopté un document de synthèse sur les règles et les normes détaillées exposées à l'annexe de la principale proposition. Dans ces documents, le groupe a souligné, en s'inspirant du point de vue exprimé par le CEPD dans ses avis, que le troisième pilier manquait d'un cadre général solide en matière de protection des données et a prôné l'adoption de règles claires concernant la supervision indépendante, la limitation des finalités et les transferts vers des pays tiers.
- en ce qui concerne les négociations relatives à la décision-cadre sur la protection des données relevant du troisième pilier, le groupe de travail « Police et Justice » s'est inquiété du fait que le champ d'application de cet instrument soit limité et qu'il ne soit pas prévu d'instituer une

<sup>(63)</sup> DubliNet est le réseau électronique sécurisé de moyens de transmission entre les autorités nationales qui traitent les demandes d'asile. En principe, un résultat positif dans Eurodac déclenche un échange de données relatives au demandeur d'asile, qui est réalisé par l'intermédiaire de DubliNet.

- enceinte consultative des autorités de contrôle nationales et européennes pour garantir l'application harmonisée de ses dispositions ;
- le groupe a également examiné la question des dossiers passagers, en liaison avec le Groupe Article 29, et a contribué à la discussion lancée par la Commission européenne sur le nouveau programme pluriannuel dans le domaine de la liberté, de la sécurité et de la justice.

#### 4.5. Conférence européenne

Les autorités chargées de la protection des données des États membres de l'UE et le 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 faire part de leur expérience sur différents sujets. Le CEPD et le Contrôleur adjoint ont participé à Rome, les 17 et 18 avril 2008, à la conférence organisée par l'autorité italienne de la protection des données et intitulée. « *Garanties pour la protection des données à caractère personnel* », le thème général étant « Quelles perspectives pour la protection de la vie privée en Europe et au-delà ? »

La conférence a examiné plusieurs nouvelles tendances dans le domaine de la sécurité et des nouvelles technologies. L'accent mis sur la gestion des frontières transparaît dans une déclaration<sup>(64)</sup> adoptée par la conférence à propos de trois communications de la Commission européenne à ce sujet. Cette déclaration préconise d'évaluer l'efficacité des mesures existantes avant d'en prendre de nouvelles qui limiteraient les droits et les libertés des voyageurs. Par ailleurs, la conférence s'est également penchée sur des sujets très concrets, par exemple la protection des données concernant les enfants et l'expérience de sensibilisation menée dans les écoles portugaises. Le CEPD est intervenu à propos des nouveaux défis auxquels les entités chargées de la protection des données sont confrontées et des opportunités offertes par le traité de Lisbonne.

Juste avant la conférence, un atelier a eu lieu pour faire le point sur l'évolution de la situation en ce qui concerne l'initiative de Londres (voir le point 4.7) et d'en faire connaître les résultats à la plupart des homologues européens.

La prochaine conférence européenne aura lieu à Édimbourg les 23 et 24 avril 2009 et portera sur l'expérience acquise lors de la mise en œuvre de la directive 95/46/CE.

Des membres du personnel ont participé à des ateliers de traitement des dossiers, à Ljubljana et à Bratislava, en mars et en septembre 2008. Cet intéressant mécanisme de coopération au niveau du personnel – pour l'échange des meilleures pratiques entre les autorités européennes chargées de la protection des données – est entré dans sa dixième année. Le prochain atelier de traitement de dossiers aura lieu à Prague en mars 2009.

#### 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 régions 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 trentième conférence internationale des commissaires à la protection des données et à la vie privée, tenue à Strasbourg du 15 au 17 octobre 2008, a été accueillie conjointement par la Commission nationale de l'informatique et des libertés (CNIL) et le commissaire fédéral allemand à la protection des données et à la liberté de l'information, en coopération étroite avec le Conseil de l'Europe. Un grand nombre de délégués de quelque 60 pays du monde entier y ont participé.

Le thème général de la conférence était « protéger la vie privée dans un monde sans frontières » ; six sessions plénières ont eu lieu dans l'hémicycle du Conseil de l'Europe sur les thèmes « La vie privée : obstacle ou atout pour la croissance économique ? », « La vie privée : un espace en voie de disparition ? », « Sécurité : vers un fichier mondial d'identification ? », « Moi, Clara, ma vie privée, mon œuvre », « L'homme assisté : ange ou démon numérique ? » et « Quelles limites et quels outils pour la régulation future de la vie privée ? ». Une conférence fermée a également été organisée à l'intention des commissaires.

Le CEPD et le Contrôleur adjoint ont tous deux participé à la conférence. Le CEPD a assuré le rôle de modérateur lors de la session portant sur le thème

<sup>(64)</sup> Disponible sur le site Internet du CEPD, onglet « Coopération », section « Conférence internationale ».



Conférence internationale des commissaires à la protection des données et de la vie privée (Strasbourg, du 15 au 17 octobre 2008).

« Quelles limites et quels outils pour la régulation future de la vie privée ? » et a présenté un rapport sur l'initiative de Londres lors de la conférence fermée.

Dans ses conclusions, la conférence a souligné la nécessité, à l'heure de la mondialisation, de règles contraignantes en matière de protection des données. Faute de telles règles contraignantes s'appliquant à tous les intervenants à l'échelle internationale, il ne sera pas possible de relever les défis du futur en matière de protection de la vie privée. Les délégués ont prôné un renforcement de la coopération internationale entre les autorités chargées de la protection des données et ont souligné que la protection des données devait figurer en bonne place dans les politiques menées par les institutions publiques et privées. Les particuliers doivent disposer de moyens appropriés pour protéger leur vie privée.

La conférence a adopté plusieurs résolutions sur les nouvelles technologies ou la nécessité de nouer un dialogue international <sup>(65)</sup> :

- résolution sur la vie privée des enfants en ligne ;

- résolution sur la protection de la vie privée dans les services de réseaux sociaux ;
- résolution visant la mise en place d'une journée ou d'une semaine internationale de la protection de la vie privée et des données personnelles ;
- résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles.

La conférence a également prévu la création d'un comité directeur relatif à la représentation de la conférence internationale lors de réunions des organismes internationaux.

La prochaine conférence internationale se tiendra à Madrid du 11 au 13 novembre 2009 et sera accueillie par l'autorité espagnole de la protection des données (*Agencia de Protección de Datos*).

#### 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

<sup>(65)</sup> Disponibles sur le site internet du CEPD, onglet « Coopération », section « Conférence internationale ».

des données du monde entier, a été présentée lors de la 28<sup>ème</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>(66)</sup>.

Plusieurs ateliers ont été organisés, dans le contexte de l'initiative de Londres, afin d'échanger des expériences et de partager les meilleures pratiques dans différents domaines, par exemple la communication, la mise en œuvre de la réglementation et la planification stratégique.

En mai 2008, le commissaire à la protection de la vie privée du Canada a organisé à Montréal un atelier consacré aux questions liées à la gestion au sein des autorités chargées de la protection des données. Il s'agissait de la première occasion d'examiner conjointement la gestion des ressources humaines (formation et expertise) et financières (modèles de financement), les modalités selon lesquelles l'efficacité peut être garantie (gestion opérationnelle et structure de gestion) ainsi que la gestion des relations extérieures (responsables de la protection de la vie privée, société civile et réseaux régionaux).

En octobre 2008, le CEPD a présenté un aperçu de l'état d'avancement de l'initiative de Londres lors de la conférence fermée tenue dans le cadre de la trentième conférence internationale de Strasbourg.

Il est probable que des ateliers d'échange des meilleures pratiques continuent d'être organisés en 2009 sur le thème de la réponse à apporter aux violations de la sécurité.

<sup>(66)</sup> Voir rapport annuel de 2006, points 4.5 et 5.1.

## 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 organisations 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 la matière.

L'organisation d'un troisième atelier est actuellement à l'étude. Il sera probablement organisé à la fin de 2009 ou au début de 2010 et portera notamment sur le recours responsable aux données biométriques dans divers contextes.

## 5. Communication

### 5.1. Introduction

L'information et la communication jouent un rôle essentiel pour assurer la visibilité des principales activités du CEPD, mieux faire entrevoir le travail accompli par ce dernier et accroître la sensibilisation à la protection des données en général. Ce rôle est d'autant plus stratégique que le CEPD est encore une institution relativement récente et qu'il convient donc de mieux faire connaître son rôle au niveau de l'UE.

Si l'on observe la période écoulée depuis la première année d'activité du CEPD jusqu'à 2008, dernière année couverte par le premier mandat, on peut prendre pleinement la mesure du chemin parcouru. Un des objectifs expressément poursuivis par le CEPD dans le cadre de ses activités de communication au cours de ses premières années d'existence était d'augmenter sa visibilité au niveau européen. Dans un délai relativement court, un travail important a été accompli en ce sens. S'appuyant sur les méthodes génériques mises en œuvre au cours de la première année, une stratégie de l'information a été conçue selon les modèles traditionnels : création d'un style maison facilement reconnaissable (logo, identité visuelle), établissement d'objectifs généraux et plus spécifiques, identification des publics concernés par les principales activités du CEPD (voir le point 5.2) et sélection d'outils de communication adaptés à chacun des groupes cibles envisagés. Les travaux ultérieurs ont essentiellement été consacrés à la conception d'une série d'outils et de pratiques de communication habituellement mis en œuvre par la plupart des organismes publics (par exemple site web, bulletin d'information, brochures, documents informatifs, participation à des conférences et allocutions dans ce cadre, communiqués de presse, conférences de presse, organisation de manifestations de sensibilisation). Parallèlement, un service de presse a été créé et chargé de la communication externe via les médias (voir point 5.4).

Cinq ans après le début des travaux, on peut constater que l'accent mis sur la communication, y compris l'approche ciblée et le développement d'outils et de canaux de communication, a donné de bons résultats en termes de visibilité. Parmi les indicateurs significatifs de ces résultats positifs figurent notamment l'augmentation du nombre des demandes d'information et d'avis, l'accroissement du trafic sur le site web, la progression constante du nombre d'abonnés au bulletin d'information, ainsi que les demandes de visites d'étude dans les bureaux du CEPD et les invitations à intervenir à des conférences régulièrement adressées au CEPD. De même, les contacts plus systématiques avec les médias et l'augmentation importante de la couverture médiatique des activités du CEPD qui en résulte confortent l'opinion selon laquelle le CEPD est devenu une référence pour les questions relatives à la protection des données.

La visibilité accrue du CEPD dans le paysage institutionnel présente une utilité immédiate pour ses trois principaux rôles, à savoir le rôle de supervision à l'égard de l'ensemble des institutions et des organes communautaires procédant à des traitements de données à caractère personnel, le rôle consultatif vis-à-vis des institutions (Commission, Conseil et Parlement) intervenant dans la conception et l'adoption des nouveaux instruments législatifs et des nouvelles politiques susceptibles d'avoir un effet sur la protection des données à caractère personnel, et enfin le rôle de coopération avec les autorités nationales de supervision et les divers organes de supervision relevant du troisième pilier.

La coopération entre le CEPD et les délégués à la protection des données (DPD) des institutions et organes communautaires constitue un aspect particulier de la sensibilisation à la protection des données. Une coopération étroite constitue un moyen important de partager les bonnes pratiques et de travailler efficacement ensemble afin de sensibiliser

les acteurs et le personnel de l'UE aux questions relatives à la protection des données. Le CEPD souhaite renforcer cette coopération, notamment en encourageant les actions communes et les synergies, par exemple dans le contexte de l'organisation de manifestations de sensibilisation, notamment la Journée de la protection des données qui se tient le 28 janvier chaque année.

L'amélioration de la sensibilisation et de la communication en ce qui concerne les questions liées à la protection des données figurait également parmi les principaux objectifs de l'initiative de Londres (voir le point 4.7). Un des résultats importants du premier atelier, dans cette perspective, a été la création d'un réseau d'agents de communication (auquel participe le CEPD). Les autorités chargées de la protection des données y font appel pour échanger des bonnes pratiques et réaliser des projets spécifiques, comme l'élaboration d'actions conjointes lorsque certains événements ont lieu dans ce domaine.

Le projet EuroPriSe, qui vise à tester la faisabilité d'un label européen de protection des données personnelles pour les biens et les services respectueux de la vie privée, constitue une autre initiative intéressante pour améliorer simultanément la communication et la protection effective des données. Ce projet a été conçu avec succès par le « Centre indépendant du Schleswig-Holstein pour la protection de la vie privée », c'est-à-dire l'autorité régionale chargée de la protection des données à Kiel (Allemagne), en collaboration avec un certain nombre d'autres acteurs, parmi lesquels figurent plusieurs autres autorités européennes chargées de la protection des données au niveau national ou régional.

En juillet 2008, le CEPD a pu assister à la célébration du trentième anniversaire de la protection des données au Schleswig-Holstein et, à cette occasion, il a attribué à une société le premier label européen de protection des données personnelles, pour la conception d'un moteur de recherche respectueux de la vie privée. L'objectif était également d'appuyer le label européen de protection des données personnelles en tant que mécanisme important et approprié de promotion des produits et services informatiques respectueux de la vie privée. Le CEPD a également été associé à l'attribution de trois autres labels européens de protection des données personnelles lors d'un atelier EuroPriSe tenu en novembre 2008 à Stockholm <sup>(67)</sup>.

<sup>(67)</sup> Voir : « La protection des données dans le Schleswig-Holstein, en Europe et dans une société de l'information d'envergure mondiale », Kiel, 14 juillet 2008, et « Introductory remarks on Presentation of European Privacy Seals », Stockholm, 13 novembre 2008, allocutions disponibles sur le site du CEPD.



EuroPriSe, remise du premier label européen de protection des données

Le CEPD considère que le label européen de protection des données personnelles est un instrument particulièrement créatif et prometteur afin de promouvoir et de garantir une protection effective. D'une part, il cadre bien avec la notion fondamentale de « prise en compte du respect de la vie privée dès la conception », qui permet de garantir efficacement la fourniture de produits et de services informatiques respectant voire, lorsque c'est possible, améliorant la protection de la vie privée. D'autre part, il constitue une mesure incitant clairement les créateurs et les fournisseurs de ces produits et services à investir pour améliorer la protection de la vie privée et à retirer des bénéfices de ces investissements, lorsque cela est justifié. Une telle approche est manifestement aussi à l'avantage des utilisateurs et de toutes les autres personnes, qui ont le droit de prendre une décision sur ces questions en se fondant sur des informations solides.

Les points qui suivent décrivent les activités que le CEPD a menées en 2008 dans le domaine de l'information et de la communication, c'est-à-dire la participation du CEPD à des conférences et à des ateliers, le travail accompli par le service de presse et la communication externe avec les médias, le traitement des demandes d'information, le développement des outils d'information en ligne (site web et bulletin d'information) et de publications, les visites d'étude et l'organisation de manifestations de sensibilisation.

## 5.2. Caractéristiques de la communication

La politique de communication du CEPD doit être conçue en fonction de la taille, du mandat et du caractère récent de l'institution. Il convient donc de suivre une stratégie sur mesure et d'avoir recours

aux outils les plus appropriés pour cibler les publics concernés, ces outils devant pouvoir être adaptés à un certain nombre de contraintes et d'exigences.

### Principaux publics et groupes cibles

À la différence de la plupart des autres institutions et organes de l'UE, dont les politiques et les activités de communication doivent être menées à un niveau général et s'adresser à l'ensemble des citoyens de l'Union, le champ d'action direct du CEPD est beaucoup plus restreint. Il s'adresse avant tout aux institutions et aux organes communautaires, aux personnes concernées en général et au personnel de l'UE en particulier, aux acteurs politiques de l'UE ainsi qu'aux homologues du secteur 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 ». La sensibilisation des citoyens de l'UE aux questions liées à la protection des données, au niveau des États membres, repose sur 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, contribue lui aussi à mieux se faire connaître du grand public, notamment grâce à un certain nombre d'outils de communication (site internet, bulletin d'information et autres supports), en entretenant des contacts réguliers avec les parties intéressées (accueil d'étudiants dans les bureaux du CEPD, par exemple) et en participant à des événements publics, réunions et autres conférences.

### Politique linguistique

La politique de communication du CEPD doit aussi tenir compte de la nature spécifique de son champ d'activité.

Les questions liées à la protection des données peuvent être considérées comme relativement techniques et obscures pour les non-spécialistes, et le langage utilisé dans la communication doit être adapté en conséquence, surtout dans le cas d'outils d'information et de communication visant toutes sortes de public, comme le site Internet et les brochures d'information. Pour ces outils comme pour les réponses aux demandes d'informations émanant des citoyens, il convient de communiquer dans un style clair et intelligible qui évite tout jargon inutile. Des efforts constants sont donc fournis à cet effet, visant en outre à corriger l'image excessivement « juridique » du domaine de la protection des données.

Si le public visé est plus spécialisé (par exemple les médias, les experts de la protection des données, les

acteurs de l'UE), l'emploi de termes techniques et juridiques est davantage justifié. Ainsi, pour communiquer la même information, il peut être nécessaire d'adapter le format et le style au public visé (grand public / audience plus spécialisée).

### Incidence

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 », incitant en cela à éviter une communication excessive. Le recours aux outils de communication « traditionnels » (les communiqués de presse par exemple) est donc volontairement limité aux thèmes de grande importance, pour lesquels il est jugé nécessaire et opportun de réagir et d'informer le public général.

Il est également essentiel de mesurer les effets des activités de communication pour évaluer l'efficacité de l'approche suivie et, si nécessaire, réorienter l'action. Une révision de la stratégie d'information mise en place après la création du CEPD sera donc entreprise en 2009.

## 5.3. Discours

Tout au long de l'année, le CEPD a continué de consacrer beaucoup de temps et d'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, à l'occasion de discours et de contributions similaires devant différentes institutions et dans divers États membres.

Il a fréquemment participé à des réunions de la Commission LIBE du Parlement européen ou à des événements connexes. Le 21 janvier, il est intervenu lors d'un séminaire public consacré à la fusion entre Google et Double Click. Le 11 février, il a émis des observations sur le projet de cadre en matière de protection des données relevant du troisième pilier. Le 26 mars, il a présenté un avis sur les éléments de sécurité et biométriques des passeports ainsi qu'un résumé de son rapport annuel pour 2007. Le 5 mai, il a présenté son avis sur la modification de la directive concernant la protection de la vie privée dans le secteur des communications électroniques. Le 29 mai, il a participé à une table ronde sur le système d'asile instauré par le système de Dublin, en liaison avec le contrôle coordonné dans le cadre d'Eurodac. Le 2 juin, il s'est exprimé lors d'une audition consacrée à l'accès du public aux documents. Le 30 juin, il a apporté deux contributions à une table ronde sur les frontières extérieures. Le 8 septembre, il a présenté de nouvelles observations sur la révi-



Peter Hustinx prononce un discours à la Conférence internationale des commissaires à la protection des données et de la vie privée (Strasbourg, du 15 au 17 octobre 2008).

sion des directives concernant le service universel et concernant la protection de la vie privée dans le secteur des communications électroniques.

Le CEPD a également participé à d'autres réunions avec le Parlement européen. Le 26 février, il s'est exprimé devant la Commission « Emploi et affaires sociales » sur des questions relatives à la sécurité sociale. Le 14 mai, il s'est exprimé lors d'une réunion convoquée par le secrétaire général et les directeurs généraux du Parlement sur le respect du règlement (CE) n° 45/2001. Le 17 septembre, il a évoqué diverses questions liées à la modification de la directive concernant la protection de la vie privée dans le secteur des communications électroniques avec des membres du Parlement européen appartenant à différentes commissions et à différents groupes politiques. Le 6 novembre, il s'est exprimé lors d'un séminaire organisé par le service juridique du Parlement sur certaines questions récentes concernant à la fois le premier et le troisième pilier.

Le 25 mars, le CEPD a présenté son avis sur la proposition relative aux dossiers passagers de l'UE au Groupe multidisciplinaire « Criminalité organisée » du Conseil. Le 11 septembre, il a de nouveau

participé à une réunion du groupe afin de présenter ses observations sur les priorités stratégiques de la présidence française. Le 30 septembre, à Paris, il s'est exprimé lors d'une conférence sur la recherche dans le domaine de la sécurité organisée dans le cadre de la présidence française. Le 6 octobre, à Nice, il a participé à une conférence similaire sur le thème de l'internet des objets. Le 11 décembre, il s'est exprimé lors d'un séminaire consacré à l'accès du public aux documents organisé par la représentation permanente de la Finlande à Bruxelles.

Le CEPD est également intervenu auprès d'autres institutions de l'UE. Le 24 avril, le CEPD et le Contrôleur adjoint se sont rendus au Tribunal de la fonction publique, à Luxembourg, pour une séance d'information sur certaines questions concernant la protection des données. Le 12 juin, le CEPD s'est exprimé lors d'une réunion convoquée par le secrétaire général et les directeurs généraux de la Commission européenne sur le respect du règlement (CE) n° 45/2001. Le 17 décembre, à Bruxelles, le CEPD et le Contrôleur adjoint sont tous deux intervenus lors d'un séminaire du CEPD, auquel participaient d'autres parties intéressées, sur le contrôle des institutions de l'UE.

Le 25 janvier, le CEPD a présenté un exposé au Collège d'Europe, à Bruges, sur les principes, les acteurs et les défis de la protection des données à caractère personnel dans l'UE. Le 26 mai, il a apporté sa contribution à une conférence sur la protection des données dans le cadre du troisième pilier organisée à l'Académie de droit européen (ERA), à Trèves. Le 10 juin, il s'est rendu à l'Institut universitaire européen (IUE) de Florence pour y présenter un exposé sur le thème « Protection des données dans l'UE dans le cadre d'une économie mondialisée : menaces et risques pour la sécurité collective et les droits de l'homme ».

À la fin janvier, le CEPD se trouvait aux États-Unis pour un programme de réunions avec des fonctionnaires fédéraux et d'autres parties intéressées par la protection de la vie privée. Le 28 janvier, il a participé à une conférence tenue à la Duke University (Durham, Caroline du Nord) à l'occasion de la « journée de la protection des données ». Le 29 janvier, il s'est exprimé à l'université de Georgetown (Washington DC). Le 30 janvier, il a présenté un exposé au Washington College of Law de l'American University (Washington DC). Le 31 janvier, il s'est exprimé lors de la réunion organisée par le European Institute (Washington DC).

Le CEPD a également participé à plusieurs réunions avec des membres des parlements nationaux. Le 5 mars, à Londres, il a témoigné devant une commission de la House of Lords sur le thème de la société de la surveillance. Le 20 mars, il a participé à un séminaire sur les questions relatives à la vie privée organisé par la commission de la justice du sénat néerlandais. Le 2 avril, à Bruxelles, il est intervenu devant une sous-commission de la House of Lords sur le thème des dossiers passagers de l'UE. Le 4 avril, à Lyon, il s'est exprimé, lors du sixième colloque parlementaire Paris-Berlin consacré à la sécurité collective et aux libertés individuelles, sur le thème du juste équilibre entre la sécurité, la mobilité et la protection de la vie privée.

Pendant l'année, le CEPD s'en est rendu dans plusieurs États membres à diverses occasions. Le 23 janvier, il s'est exprimé lors d'une conférence sur les données biométriques à l'Institut d'études politiques de Paris. Le 15 février, à La Haye, il s'est exprimé devant une commission consultative du parlement néerlandais sur la sécurité et la protection de la vie privée. Le 3 mars, à l'université Erasmus de Rotterdam, il a prononcé une allocution pour les étudiants en droit. Le 28 avril, il a présenté son document stratégique intitulé « Le CEPD et la

recherche et le développement technologique dans l'UE » à l'Institut für Technikfolgen-Abschätzung de Vienne. Le 6 mai, lors de la neuvième conférence de Berlin sur la protection des données, il s'est exprimé sur le thème « Défis stratégiques pour la protection des données en Europe ». Le 28 mai, il a participé à un groupe de discussion à la Chambre de commerce internationale à Paris. Le 6 juin, il a prononcé une allocution sur les péages routiers lors d'une conférence sur les systèmes de transport intelligents tenue à Genève. Le 20 juin, il s'est exprimé sur le thème de la protection des données dans l'UE dans les bureaux de l'autorité hongroise de la protection des données, à Budapest. Le 14 juillet, il a assisté au trentième anniversaire de la protection des données au Schleswig-Holstein et prononcé un discours à Kiel (voir aussi le point 5.1).

Le 16 septembre, il s'est exprimé lors d'un sommet des avocats de société. Le 23 septembre, il a participé à un débat public sur des questions relatives à la protection de la vie privée qui s'est tenu à Amsterdam. Le 25 septembre, il a prononcé une allocution lors d'une conférence organisée à Bruxelles par la section internationale de l'Association du barreau américain. Le 11 octobre il a apporté sa contribution lors d'une « Challenge conference » organisée à Paris sur le thème de la sécurité et de la protection de la vie privée. Le 22 octobre, il s'est exprimé lors de la conférence « Biométrie 2008 » à Londres. Le 27 octobre, lors d'une « RSA Conference » tenue à Londres, il s'est exprimé sur les violations de la sécurité informatique et sur des questions relatives à la vie privée et aux communications électroniques. Le 2 décembre, il est intervenu à l'occasion d'une conférence sur la gestion des frontières organisée à Bruxelles. Le 3 décembre, il a abordé la question de la « proportionnalité » lors d'une conférence organisée à Londres sur le thème de la justice. Le 9 décembre, à Ispra, lors d'une réunion d'un sous-groupe du Forum européen de la recherche et de l'innovation en matière de sécurité, il s'est exprimé à propos de la recherche en matière de sécurité et de protection de la vie privée.

Le Contrôleur adjoint de la protection des données a présenté des exposés similaires. Le 11 avril, au *Centre d'étude* du gouvernement catalan, il a consacré une présentation à l'incidence de la protection des données sur les procédures judiciaires. Le 6 mai, lors d'un séminaire international organisé par l'autorité catalane de la protection des données, il s'est exprimé sur la question des tensions entre sécurité et protection des données. Le même jour à Barcelone, et le 7 mai à Madrid, pour un groupe de

conseillers juridiques, il a prononcé une allocution sur les modifications qui pourraient être apportées aux directives de l'UE en matière de protection des données. Le 20 mai, à Madrid, lors d'un séminaire de formation pour les juges et les procureurs, il a donné une présentation consacrée à l'incidence de la protection des données dans le cadre des procédures civiles. Le 22 mai, il s'est exprimé sur la nouvelle décision-cadre relative à la protection des données lors d'un séminaire international de juges et de procureurs organisé à Tolède.

Le 9 septembre, à Budapest, lors de la conférence annuelle des entreprises européennes spécialisées dans la destruction des données, il s'est exprimé sur la question de la conservation, de l'effacement et des mesures de sécurité concernant les données à caractère personnel. Le 4 octobre, il a présenté le nouveau Système européen d'information sur les casiers judiciaires (ECRIS) lors de la conférence annuelle de la European Criminal Bar Association, à Bratislava. Le 7 octobre, à Bruxelles, lors d'un séminaire organisé par le groupe ALDE/ADLE du Parlement européen, il a consacré un exposé aux défis à venir dans le domaine de la protection des données. Le 28 octobre, à Grenade, il s'est exprimé au sujet des données médicales lors d'une réunion du réseau andalou de la santé publique. Le 25 novembre, à Bruxelles, il a présenté un exposé sur l'incidence des nouvelles technologies dans le domaine de la sécurité lors d'un séminaire organisé par le Centre d'études de la politique européenne (CEPS). Le 3 décembre, à Bilbao, il s'est exprimé sur la protection des données et l'information judiciaire lors d'un atelier organisé par le tribunal supérieur de justice (« tribunal superior de justicia ») du pays basque. Le 12 décembre, à La Haye, il s'est exprimé sur l'équilibre entre la sécurité et la protection des données lors de la septième conférence annuelle du Réseau international du droit pénal.



L'équipe d'information.

## 5.4. Relations avec les médias

### Service de presse

Le service de presse est chargé de la communication externe avec les médias, assurée grâce à des contacts réguliers avec les journalistes. Il est également chargé de traiter les demandes d'informations et de conseils présentées par la presse, des acteurs intéressés ou des citoyens, de rédiger les communiqués de presse et les bulletins d'information, et d'organiser les conférences de presse, visites d'étude et entretiens avec le CEPD ou le Contrôleur adjoint. En outre, la responsable de l'information et de la presse dirige une équipe d'information de nature flexible qui fournit une aide pour les activités menées dans ce domaine et participe aux manifestations promotionnelles (notamment la « Journée européenne de la protection des données » et la Journée portes ouvertes de l'UE, voir le point 5.9).

### Contacts avec les médias

Le CEPD entend être aussi accessible que possible pour les journalistes, de façon à ce que le public puisse suivre son travail. Il informe régulièrement les médias, surtout par des communiqués de presse, des interviews, des discussions de fond et des conférences de presse. La gestion des demandes formulées par les médias (demandes d'informations ou d'avis), telles que le CEPD en reçoit régulièrement sur des questions qui intéressent le grand public, permet de renforcer les contacts avec les médias.

En 2008, le service de presse a publié 13 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 particulier pour le public. Ces questions concernaient notamment le système envisagé de gestion des frontières extérieures de l'UE, les données biométriques dans les passeports, le réexamen de la directive relative à la vie privée et aux communications électroniques, l'accès du public aux documents de l'UE, l'échange d'informations à des fins répressives au niveau transatlantique ainsi que l'adoption de la décision-cadre concernant la protection des données dans le troisième pilier. Les communiqués de presse sont publiés en anglais et en français sur le site du CEPD ainsi que dans la base de données interinstitutionnelle des communiqués de presse gérée par la Commission (RAPID). Ils sont diffusés auprès d'un réseau régulièrement mis à jour de journalistes et d'acteurs concernés. Les informations fournies dans ces communiqués font généralement l'objet d'une couverture médiatique



Peter Hustinx et Joaquín Bayo Delgado présentent leur rapport annuel 2007 à la presse.

significative. Elles sont régulièrement reprises dans la presse générale et spécialisée, et publiées sur des sites web institutionnels et autres, représentant notamment les institutions et organes européens, des ONG, des instituts universitaires et des sociétés du secteur des technologies de l'information.

En 2008, le CEPD a donné quelque 25 interviews à des journalistes de la presse écrite, de la radiotélévision et des médias électroniques en Europe et dans des pays tiers. Plusieurs articles et extraits d'interviews ont été publiés dans la presse nationale (par exemple *Daily Telegraph*, *BBC*, *New York Times*, divers journaux allemands et néerlandais, ainsi que l'agence de presse hongroise), internationale et européenne (par exemple *The Economist*, *European Voice*, *Euractiv*), et sur des sites web spécialisés dans le domaine de la protection des données et des questions informatiques. En outre, plusieurs interviews ont été données à la radio et à la télévision (par exemple Deutsche Welle, télévision néerlandaise, Radio 1 RAI, radio polonaise). Les interviews ont porté sur des sujets tels que les dossiers passagers de l'UE, la directive sur la conservation des données, le système de gestion des frontières envisagé par l'UE, le programme d'exemption de visa (Visa Waiver

Program) des États-Unis, le système d'information de Schengen (SIS), la protection de la vie privée dans le secteur de la santé et la question de savoir si la protection des données est garantie de manière adéquate au niveau de l'UE.

## 5.5. Demandes d'informations

Le nombre de demandes d'informations ou de conseils adressées par le grand public est passé à plus de 180 en 2008 (par rapport à 160 en 2007). Ces demandes 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 de la vie privée ou des données et dans le secteur informatique (cabinets juridiques, consultants, groupes de pression, ONG, associations, universités, etc.) aux citoyens souhaitant obtenir plus d'informations sur des questions relatives à la protection de la vie privée ou qui demandent une assistance pour résoudre les questions ou problèmes auxquels ils sont confrontés dans ce domaine. Ces demandes sont essentiellement reçues sur la boîte électronique fonctionnelle du CEPD et, moins fréquemment, par courrier postal.

Les demandes d'informations recouvrent une large catégorie de demandes comprenant des questions générales sur les politiques et la législation en matière de protection des données, *tant dans* l'UE qu'à l'échelon national, mais également sur des questions plus précises et plus techniques sur un aspect donné de la protection de la vie privée et des données personnelles. En 2008, des demandes d'information ont par exemple été reçues concernant des incidents de sécurité liés à des atteintes aux données, les technologies biométriques, l'identification par radiofréquence, la protection de la vie privée sur Internet – y compris les réseaux sociaux, le contrôle des communications électroniques et l'enregistrement des appels – ainsi que le traitement des images, le lancement de Google Street View, la révision du paquet télécom de l'UE, le transfert des données à caractère personnel vers des pays tiers, ainsi que les dispositions du traité de Lisbonne relatives à la protection des données à caractère personnel.

Il convient de relever qu'un grand nombre de demandes d'information adressées par le public concernent des questions nationales pour lesquelles le CEPD n'est pas compétent. Dans ce cas, une réponse est envoyée décrivant le mandat du CEPD et conseillant au destinataire de s'adresser à l'autorité compétente, généralement l'autorité chargée de la protection des données dans l'État membre concerné.

Les demandes qui vont au-delà des aspects purement informatifs et qui exigent donc une analyse plus approfondie sont habituellement confiées à des gestionnaires de dossiers. En 2008, les questions traitées ont concerné par exemple les dossiers passagers, le SIS, la protection des données dans le contexte transatlantique, les données biométriques dans Eurodac, la protection des données dans le cadre de poursuites pénales, les règles d'entreprise contraignantes ainsi que l'interface entre la protection des données et la législation en matière de concurrence.

Comme lors des années précédentes, la plupart des demandes étaient rédigées en anglais et, dans une moindre mesure, en français, en allemand, en italien et en espagnol. Le service de presse a pu ainsi répondre rapidement, dans le délai imparti de 15 jours ouvrables. Pour les demandes plus rares rédigées dans d'autres langues officielles de l'UE, il a fallu faire appel au service de traduction du Conseil.

## 5.6. Visites d'étude

Dans le cadre des efforts fournis pour renforcer sa visibilité et l'interaction avec le monde universitaire,

le CEPD accueille régulièrement des groupes d'étudiants, spécialisés notamment dans les domaines du droit européen, de la protection des données et/ou de la sécurité des technologies de l'information. Ainsi, en mars 2008, le CEPD a accueilli un groupe d'étudiants de l'université de Tilburg spécialisés dans le droit international et européen.

D'autres groupes de visiteurs ont également été reçus dans les bureaux du CEPD, notamment, en mai 2008, une délégation de la Commission de la justice du parlement néerlandais. L'association danoise « IT Pol » (association de collecte d'information sur les technologies de l'information à destination du monde politique) a également rendu visite au CEPD en février afin de discuter des implications pour la protection de la vie privée et des données des récentes initiatives en matière de conservation des données et de surveillance.

## 5.7. Outils d'information en ligne

### Site web

Le site web reste l'outil de communication et d'information le plus important du CEPD. C'est aussi sur le site web que les visiteurs peuvent accéder à l'ensemble des différents documents élaborés dans le cadre des activités du CEPD (avis relatifs à des contrôles préalables et propositions d'actes législatifs européens, observations, priorités de travail, publications, discours, communiqués de presse, bulletin d'information, informations sur les événements, etc.). Le site web est par conséquent mis à jour quasi quotidiennement par la publication des documents et informations utiles.

### Évolution du contenu

Comme annoncé dans le rapport annuel pour 2007, les outils d'information ont été enrichis en 2008 en vue d'améliorer le contenu du site web et de mieux répondre aux attentes des visiteurs.

Parmi ces améliorations figure la création d'un glossaire en rapport avec la protection des données à caractère personnel. Il comprend 75 termes accompagnés de liens vers des informations complémentaires figurant sur des pages internes et externes au site web du CEPD. L'objectif de ce glossaire est surtout d'aider les visiteurs du site à mieux appréhender les activités et le travail accomplis par le CEPD ainsi que les questions relatives à la protection des données d'une manière plus générale. Parallèlement, une section « Questions – Réponses » a été créée. L'objectif était notamment de mieux expliquer le

mandat, les compétences et le domaine d'action du CEPD et de fournir un guide rapide répondant aux questions les plus fréquentes. Cette section présente des informations de fond et des conseils pratiques sur des questions telles que les fonctions et les compétences du CEPD, la législation de l'UE en matière de protection des données, les droits de la personne concernée, les règles régissant le traitement des données à caractère personnel ainsi que le transfert de ces données.

La publication de ces deux nouvelles sections sur le site web est prévue pour le début de l'année 2009. En complément de la section « Questions – Réponses », un document de type « Foire aux questions » est également en cours d'élaboration afin de fournir des réponses ciblées à des profils spécifiques et à des publics concernés (par exemple le personnel de la CE, les visiteurs, les personnes qui postulent à un poste vacant dans les institutions et les organes communautaires).

#### *Évolution technique*

Pour améliorer les performances du site web du CEPD, lancé en 2007, des améliorations techniques ont été apportées en 2008 en vue de faciliter la navigation. Les pages concernées étaient celles comprenant un grand nombre de documents, notamment la page présentant la liste des avis du CEPD concernant les contrôles préalables, qui devait être réorganisée et scindée pour que le site web fonctionne correctement.

Outre l'amélioration du fonctionnement général du site web, une fonction de « recherche avancée » a été ajoutée. Cette nouvelle fonction permet aux visiteurs de combiner les critères pour effectuer des recherches précises dans les documents en format PDF. La fonction de recherche avancée devra néanmoins être ajustée en 2009 afin qu'elle fournisse des résultats plus approfondis.

Un outil statistique fournissant des données relatives au trafic et à la navigation a été mis en place en janvier 2008. Il ressort des statistiques que, du 1<sup>er</sup> février au 31 décembre 2008, le site web a reçu 81 841 visiteurs au total, avec un maximum de 10 095 visiteurs en mai au moment de la publication du rapport annuel pour 2007. Outre la page d'accueil et la fonction de recherche avancée, les pages le plus souvent consultées sur le site ont été celles consacrées aux actualités, aux communiqués de presse et aux rapports annuels.

Dans le cadre du Comité éditorial interinstitutionnel « Internet », le webmestre du CEPD a continué

de participer aux discussions sur la création d'un outil de recherche interinstitutionnel de l'UE qui devrait, ultérieurement, être disponible sur le site web Europa.

En 2009, le site web sera mis à jour pour tenir compte de la nomination du Contrôleur et du Contrôleur adjoint pour le deuxième mandat. Des nouveautés techniques, concernant en particulier la fonction de recherche avancée, ainsi que des améliorations de la présentation sont également en préparation. En outre, une étude sera lancée sur une éventuelle refonte de la page d'accueil pour la rendre plus dynamique, une importance accrue étant accordée aux dernières nouvelles concernant les activités du CEPD.

#### **Newsletter**

La « newsletter » du CEPD reste un outil efficace pour mieux faire connaître les dernières activités du CEPD et attirer l'attention sur les ajouts récents au site web. Elle présente les nouvelles concernant les avis rendus par le CEPD sur des propositions législatives européennes et sur des contrôles préalables, des informations sur les événements et les conférences à venir dans le domaine de la protection des données, ainsi que les discours et interventions du CEPD. Les newsletters sont disponibles sur le site web du CEPD. Une fonction d'abonnement automatique figure sur la page pertinente.

Cinq numéros de la newsletter du CEPD ont été publiés en 2008, soit en moyenne un tous les deux mois. La newsletter est publiée en anglais et en français.

Le nombre d'abonnés est passé de 635 personnes à la fin de 2007 à un total de 880 personnes à la fin de 2008. Parmi les abonnés figurent notamment des membres du Parlement européen, du personnel de l'UE et 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.

En raison de cette augmentation régulière du nombre d'abonnés, une nouvelle version de la newsletter, plus conviviale, est en préparation. Il s'agit de repenser l'organisation de la newsletter afin d'en améliorer la lisibilité.

À cette fin, des travaux préparatoires ont été entrepris en 2008 avec une agence de communication spécialisée dans la publication d'informations, afin de recenser les besoins et d'envisager la marche à suivre. Les travaux se poursuivront en 2009 pour mener le projet à terme.

## 5.8. Publications

### Rapport annuel

Le rapport annuel constitue la principale publication du CEPD. Publié normalement au printemps, il présente un aperçu des activités du CEPD au cours de l'année concernée dans les principaux domaines opérationnels que sont la supervision, la consultation et la coopération. Il décrit en outre les réalisations en termes de communication externe et l'évolution de la situation en ce qui concerne l'administration, le budget et le personnel.

Le rapport peut présenter un intérêt particulier pour différents groupes et différentes personnes aux niveaux international, européen et national : les personnes concernées en général, et les agents de la CE en particulier, le système institutionnel de l'UE, les autorités chargées de la protection des données, les spécialistes, groupes d'intérêt et ONG actifs dans ce domaine, ainsi que les journalistes et toute personne recherchant des informations sur la protection des données personnelles au niveau de l'UE.

Le 26 mars 2008, le CEPD a présenté son rapport annuel pour 2007 à la Commission LIBE du Parlement européen.

Une conférence de presse a été organisée à la mi-mai pour présenter le rapport à la presse. La conférence de presse a permis de mettre l'accent sur les conséquences du traité de Lisbonne en ce qui concerne le renforcement de la protection des données personnelles. Le CEPD a profité de l'opportunité pour souligner que le nouveau traité devait être considéré comme une occasion pour l'administration de l'UE de démontrer qu'une protection effective des données personnelles est une des valeurs fondamentales à la base des politiques de l'UE.

### Brochure d'information

Afin de mieux faire connaître la nouvelle institution, deux brochures sur le CEPD ont été conçues après l'établissement de l'institution en 2004. L'une présente le CEPD d'un point de vue institutionnel, l'autre décrit les droits des personnes au sujet desquelles des données sont traitées par les institutions et les organes communautaires.

L'élaboration d'une brochure d'information actualisée, fusionnant les deux brochures existantes, a été initiée en 2008, notamment dans la perspective de l'expiration du premier mandat du CEPD en janvier 2009. Cette mise à jour sera en outre l'occasion de concevoir une brochure modernisée. Ce nouveau matériel d'information mettra en lumière,

dans un style éditorial plus dynamique et direct, les points essentiels concernant le CEPD, la protection des données personnelles au niveau de l'UE et des informations pratiques.

## 5.9. Actions de sensibilisation

Participer à des événements dans le cadre des activités 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 aux organes communautaires dans le domaine de la protection de la vie privée et des données.

### Journée de la protection des données

Les États membres du Conseil de l'Europe et les institutions européennes ont célébré le 28 janvier 2008 la deuxième journée de la protection des données. Cette date marque l'anniversaire de l'adoption, en 1981, de la Convention 108 du Conseil de l'Europe, premier instrument international juridiquement contraignant en matière de protection des données.

Cette manifestation a été l'occasion pour le CEPD de mettre l'accent sur la sensibilisation des agents de l'UE et de toutes les personnes intéressées au sujet de leurs droits et obligations en matière de protection des données. À cet effet, un stand d'information a été ouvert dans les bâtiments du Parlement européen, de la Commission et du Conseil pendant trois jours consécutifs. Le CEPD a présenté les rôles qui lui incombent en matière de supervision, de consultation et de coopération, ainsi que ses réalisations et ses activités en cours. Le stand du CEPD a été



Le stand du CEPD à la Commission européenne lors de la Journée de la protection des données (Bruxelles, 30 janvier 2008).

créé en coopération avec les délégués à la protection des données des institutions concernées, qui présentaient également leurs activités.

Au total, l'équipe du CEPD a accueilli quelque 250 visiteurs. Différents supports d'information présentant le travail accompli par le CEPD ont été distribués, de même qu'une série d'objets promotionnels. Les visiteurs ont également eu l'occasion de tester leurs connaissances dans le domaine de la protection des données en répondant à un jeu-concours rapide, et ont pu prendre part à un tirage au sort.

En vue de la prochaine journée européenne de la protection des données, l'objectif est de renforcer cette action, en particulier par une coopération plus étroite avec le réseau des délégués à la protection des données et un élargissement de l'offre de supports d'information.

#### Journée portes ouvertes de l'UE

Le 7 juin 2008, le bureau du CEPD a également participé, comme chaque année désormais, à la Journée portes ouvertes des institutions européennes, organisée au Parlement européen à Bruxelles.

Le CEPD disposait d'un stand situé dans le bâtiment principal du Parlement européen et des membres de son équipe étaient sur place pour répondre aux questions posées par les visiteurs sur le rôle du CEPD et les activités qu'il mène.

Différents supports d'information présentant les travaux du CEPD ont été distribués aux visiteurs, ainsi que des objets promotionnels. Un jeu-concours concernant le rôle du CEPD et la protection des données au niveau communautaire était



Le stand du CEPD au Parlement européen lors de la Journée portes ouvertes de l'UE (Bruxelles, 7 juin 2008).

également proposé sur place et les visiteurs avaient l'occasion de participer à un tirage au sort suivi d'une remise de prix.

#### 5.10. Priorités pour 2009

En 2009, les activités d'information et de communication que mène le CEPD porteront essentiellement sur les priorités qui suivent :

- **poursuivre le développement du site web** : outre la publication de nouveaux contenus, des améliorations techniques et graphiques seront apportées en vue de faciliter la navigation, de rendre les informations présentées visuellement plus attrayantes et de donner plus de visibilité à la section « Actualités ». Certaines parties du site devront également être mises à jour suite de la nomination du CEPD et du Contrôleur adjoint pour le deuxième mandat (2009-2014) ;
- **achever la nouvelle version de la « newsletter »** pour offrir aux lecteurs un outil d'information plus convivial ;
- **finaliser la nouvelle brochure d'information** concernant le CEPD et la protection des données personnelles dans les institutions et les organes communautaires ;
- **continuer de clarifier les compétences du CEPD** : parmi les citoyens qui ont entendu parler du CEPD, un certain nombre ne sont pas au fait de ses compétences et ont tendance à le considérer comme une sorte d'organe « chapeau » de la protection des données, auquel on peut s'adresser lorsque l'on rencontre des problèmes au niveau national. Il convient de lever ce malentendu. Une première étape consistera à clarifier le rôle du CEPD dans la nouvelle brochure d'information et sur le site web, notamment dans la section « Questions – Réponses » ;
- **rationaliser la politique du CEPD vis-à-vis de la presse**, notamment en ce qui concerne la publication des communiqués de presse et la gestion des demandes d'information, d'interviews, d'observations, etc. adressées par les médias. Des lignes directrices internes seront formalisées au sujet de la publication des communiqués de presse. Les modalités de traitement par le CEPD des demandes adressées par la presse seront également clarifiées afin d'indiquer de quelle manière et par quels canaux ces demandes doivent être présentées.

## 6. Administration, budget et personnel

### 6.1. Introduction

En vue de consolider davantage le bon démarrage du CEPD et de lui permettre ainsi de traiter les nouvelles tâches qui lui ont été assignées, des ressources supplémentaires lui ont été attribuées, tant au niveau de son budget (qui est passé de 4 955 726 EUR en 2007 à 5 307 753 EUR en 2008) que de son personnel (de 29 personnes en 2007 à 33 personnes en 2008).

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 de nouvelles règles <sup>(68)</sup> internes 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.

**La coopération avec d'autres institutions** (le Parlement européen, le Conseil et la Commission européenne) s'est encore améliorée, ce qui a permis de réaliser des économies d'échelle significatives.



Unité « Personnel, budget et administration ».

<sup>(68)</sup> Une liste des accords et décisions de nature administrative figure à l'annexe I.

### 6.2. Budget

Le budget adopté par l'autorité budgétaire pour l'exercice 2008 s'élevait à 5 307 753 EUR, ce qui représente une augmentation de 7,1 % par rapport au budget 2007.

En 2008, une nouvelle terminologie budgétaire a été appliquée. Elle se fonde sur les précédentes 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.

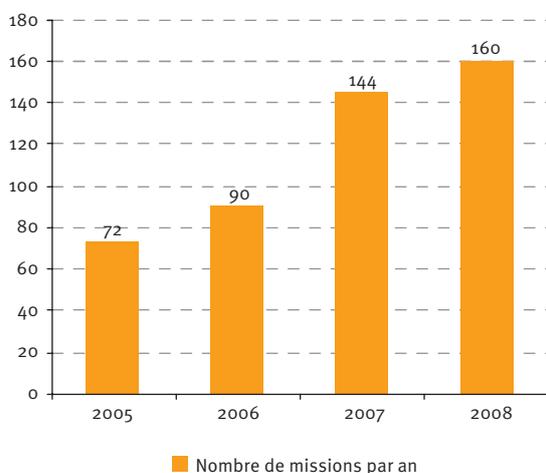
Le CEPD applique les règles internes de la Commission relatives à l'exécution du budget, dans la mesure où celles-ci sont applicables à la structure et à la taille de l'organisation, et où des règles spécifiques n'ont pas été définies. L'adoption d'une nouvelle décision qui tient compte de l'augmentation du nombre de dossiers financiers a permis d'améliorer sensiblement la structure et l'archivage des documents financiers. L'utilisation de la nouvelle terminologie budgétaire assure une transparence permanente et un traitement souple.

Plusieurs processus de traitement interne ont été optimisés afin que l'institution puisse s'adapter au nombre croissant de dossiers financiers à traiter.

**La Commission** a continué à fournir une assistance, en particulier dans le domaine de la comptabilité, le comptable de la Commission ayant également été désigné comptable du CEPD.

Dans son rapport concernant l'exercice 2007, 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. Les avis du CEPD relatifs aux



Évolution du nombre de missions

propositions législatives législatives sont traduits dans les 23 langues officielles de l'Union européenne. Ils sont publiés au Journal officiel de l'Union européenne. Depuis 2005, le nombre d'avis et d'autres documents à traduire ont connu une augmentation constante. Les avis sur les contrôles préalables et d'autres documents publiés sont en général uniquement traduits dans les langues de travail du CEPD.

Le nombre de missions effectuées par les membres et le personnel du CEPD a doublé depuis 2005, ce qui est une conséquence logique de l'augmentation des activités de l'institution. Le CEPD gère les aspects financiers des missions avec l'aide de l'Office des paiements (PMO).

### 6.3. Ressources humaines

Le CEPD bénéficie de l'aide 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 trente-trois membres du personnel).

#### 6.3.1. Recrutement

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 2008 a été décrite dans les chapitres précédents. Les ressources humaines ont un rôle fondamental à jouer dans ce contexte.

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 et une formation satisfaisante des nouveaux collègues. Le CEPD a donc demandé la création de seulement quatre postes en 2008 (trois administrateurs et un assistant). L'autorité budgétaire ayant accédé à cette demande, le tableau des effectifs est passé de vingt-neuf personnes en 2007 à trente-trois en 2008. Les avis de vacance ont été publiés au début de l'année 2008 et tous les postes ont été pourvus au cours de l'année.

La Commission, et plus particulièrement le PMO et le service médical, ont à cet égard fourni une aide précieuse.

Le CEPD a accès aux services offerts par l'Office européen de sélection du personnel (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 universitaires la possibilité de mettre en pratique les connaissances acquises durant leurs études, et d'acquérir ainsi une expérience pratique en participant aux activités du CEPD. Le CEPD 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 principal programme de stages, des dispositions spécifiques ont été prévues pour accueillir des étudiants des universités et des étudiants en doctorat pour des stages de courte durée non rémunérés. La seconde partie du programme fournit 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 qu'ont les étudiants d'effectuer un stage dans le cadre de leurs études. Ces stages sont limités à des situations exceptionnelles et soumis à des critères d'admission 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 de niveau de service 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 (DG EAC) de la Commission, qui a continué à apporter un soutien précieux grâce à l'expérience de son personnel. En septembre 2008, un nouvel accord de niveau de service a été signé, lequel améliore un certain nombre de pratiques administratives, notamment en ce qui concerne le paiement des bourses et d'autres questions financières.

### 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>(69)</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 supervision, 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 direction générale Personnel et administration de la Commission fournit une aide administrative précieuse à l'organisation de ce programme.

En 2008, deux experts nationaux ont été détachés, l'un de l'autorité espagnole chargée de la protection des données et l'autre de son homologue grecque, en remplacement des experts nationaux britannique et hongrois qui les ont précédés.

<sup>(69)</sup> Décision du CEPD du 10 novembre 2005.

### 6.3.4. Organigramme

L'organigramme du CEPD est resté le même depuis 2004 : une unité, composée à présent de huit personnes, est chargée de l'administration, du personnel et du budget ; les 25 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 à la supervision et à la consultation. L'augmentation de la charge de travail a entraîné la création d'une nouvelle fonction de coordinateur. À cet effet, huit coordinateurs ont été désignés au sein des équipes chargées des tâches de consultation et de supervision, tandis que l'attaché de presse coordonne une petite équipe chargée de l'information.

Une certaine souplesse a été maintenue dans l'attribution des tâches du personnel, étant donné que les activités de l'institution sont encore en évolution.

### 6.3.5. Dialogue social

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. Celui-ci est consulté sur une série de dispositions générales d'application du statut et sur d'autres règles internes adoptées par l'institution. En 2008, le Comité du personnel a organisé diverses activités sociales pour le personnel à l'extérieur.

### 6.3.6. Formation

En 2008, le processus consistant à élargir et améliorer les connaissances, les compétences et le savoir-faire des personnes travaillant pour le CEPD, afin que chaque membre du personnel puisse contribuer avec la plus grande efficacité à la réalisation des objectifs de l'institution, s'est poursuivi. Conformément à la décision interne adoptée dans ce domaine, un plan de formation a été établi sur la base des besoins communiqués par les membres du personnel dans le cadre d'une enquête menée à cette fin.

Les principaux axes de formation recensés dans les orientations générales annexées à la décision susmentionnée sont devenus une priorité en 2008. Il s'agit notamment des formations obligatoires organisées à l'intention des personnes nouvellement recrutées ainsi que pour des fonctions spécifiques, et des cours de langues.

Conformément à l'objectif visant à développer l'excellence dans le domaine de la protection des données, les membres du personnel du CEPD ont été autorisés à participer à des formations professionnelles externes sur la sécurité des informations. La participation à des séminaires et à des séances d'information dans le domaine de la protection des données a également été encouragée.

Afin de permettre aux nouveaux arrivants de devenir autonomes et de se développer personnellement et professionnellement, un programme de parrainage a été mis en œuvre en plus de la journée d'information déjà organisée.

Le personnel du CEPD bénéficie des cours de formation organisés par d'autres institutions européennes (Commission européenne et Parlement européen) et organes interinstitutionnels (École européenne d'Administration – EEA).

Le CEPD a continué à participer aux travaux des comités interinstitutionnels (groupe de travail interinstitutionnel de l'École européenne d'administration, comité interinstitutionnel de la formation linguistique, etc.) dans le but 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 2008, le CEPD a signé, avec les autres institutions, un nouveau protocole sur l'harmonisation des coûts des cours de langues interinstitutionnels.

### 6.3.7. Activités sociales

Une journée d'information a été mise en place à l'intention des collègues nouvellement recrutés. Durant cette journée, tous les nouveaux arrivés sont accueillis personnellement par le Contrôleur et le Contrôleur adjoint. Outre leur parrain, ils rencontrent aussi les membres de l'unité administrative, qui leur communiquent des informations sur les spécificités de l'institution et leur remettent le guide administratif du CEPD. Le CEPD travaille à un accord de coopération avec la Commission en vue de faciliter l'intégration et l'installation des nouveaux collègues, par exemple en fournissant une aide juridique pour les questions d'ordre privé (contrats de location, achat d'un logement, etc.).

Le CEPD participe, en qualité d'observateur, aux réunions du comité consultatif du Parlement européen pour la prévention et la protection au travail; en vue d'améliorer l'environnement professionnel, une réflexion a été lancée sur le bien-être au travail.

Le CEPD a continué de développer la coopération interinstitutionnelle dans le domaine des infrastructures sociales : les enfants du personnel du CEPD ont ainsi accès aux *crèches*, aux garderies et aux centres extérieurs pour enfants de la Commission, ainsi qu'aux écoles européennes. Ils ont également la possibilité de participer à la fête de Saint-Nicolas organisée par le Parlement européen.

### 6.3.8. Protocole sur les privilèges et immunités des Communautés européennes

En tant qu'autorité européenne située 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.

## 6.4 Fonctions de contrôle

### 6.4.1. Contrôle interne

#### Évaluation des risques et mise en œuvre du contrôle interne

L'évaluation des risques liés aux activités du CEPD se trouve encore à un stade peu avancé. Le CEPD a l'intention de progresser dans ce domaine en vue de maintenir au minimum le niveau de risque pour l'institution.

Entre-temps, 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.

#### Évaluation interne de l'environnement de contrôle interne

L'évaluation à laquelle ont procédé les services du CEPD a mis en évidence la fonctionnalité et l'efficacité du système de contrôle interne et a permis de formuler certaines recommandations d'amélioration. La mise en œuvre de ces recommandations a constitué une priorité en 2008. Le rapport interne sur les contrôles internes fait apparaître un taux élevé de mise en œuvre (80 %).

### Rapport annuel d'activités et déclaration d'assurance

Le CEPD a pris acte du rapport annuel d'activités et de la déclaration d'assurance jointe signée par l'ordonnateur délégué. 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 afin que l'assurance raisonnable fournie par la déclaration jointe à son rapport annuel d'activités soit effectivement étayée par des systèmes de contrôle interne appropriés.

#### 6.4.2. Audit interne

En vertu de l'accord de coopération administrative conclu en 2004 et prorogé en 2006, l'auditeur interne de la Commission a été nommé auditeur pour les services du CEPD. Sur cette base, la première visite d'audit a eu lieu en 2006 et le premier rapport d'audit élaboré par le Service d'audit interne (IAS) a été transmis en septembre 2007. Ce rapport 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 convient d'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 de l'IAS sur lesquelles le CEPD a marqué son accord a été entreprise sur la base d'un plan d'action établi au début de 2008.

En décembre 2008, l'IAS a procédé à un audit de suivi. Le rapport relatif à cet audit n'a pas encore été transmis.

#### 6.4.3. Sécurité

Conscient du niveau de confidentialité requis pour certains domaines de ses activités, le CEPD a adopté, en 2008, une décision sur les mesures applicables en matière de sécurité dans l'institution. Cette décision de portée générale définit les principes de base et les normes minimales de sécurité que tous les membres du personnel sont tenus de respecter. Elle comporte notamment des mesures concernant la gestion de

la confidentialité des informations, la sécurité des systèmes informatiques, ainsi que les conditions de sécurité des personnes et des lieux.

#### 6.4.4. Délégué à la protection des données

Le processus consistant à recenser les traitements de données à caractère personnel et à déterminer ceux qui doivent faire l'objet d'un contrôle préalable s'est poursuivi en 2008. Un inventaire des traitements internes a été achevé. Cet inventaire, conçu comme un outil pratique, vise à orienter le processus de notification. En raison de sa position spécifique, le CEPD a élaboré un système de notification simplifié pour les cas soumis au contrôle préalable.

Sur cette base, le premier processus de notification a été engagé au cours de l'année 2008. Par ailleurs, différentes déclarations de confidentialité (sous forme de communications au personnel) ont été rédigées afin de communiquer les informations visées aux articles 11 et 12 du règlement (CE) n° 45/2001.

Afin que les personnes concernées puissent exercer leurs droits, une boîte aux lettres électronique a été spécialement créée à cet effet.

La participation aux réunions du réseau des DPD a permis de partager des expériences et de discuter des questions horizontales.

### 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. Le CEPD a accueilli tous les nouveaux membres de son personnel en restructurant l'espace de travail. L'utilisation optimisée de l'espace alloué qui en a résulté a atteint sa pleine capacité en 2008.

Le CEPD a continué à gérer de manière indépendante l'inventaire de son mobilier et de ses biens informatiques, avec le concours des services du Parlement européen.

### 6.6. Environnement administratif

#### 6.6.1. Assistance administrative et coopération interinstitutionnelle

Le CEPD bénéficie de la coopération interinstitutionnelle dans de nombreux domaines administratifs

en vertu de l'accord de coopération administrative conclu en 2004 avec les secrétaires généraux de la Commission, du Parlement et du Conseil et prorogé pour une durée de trois ans en 2006. Cette coopération est extrêmement précieuse pour le CEPD en termes d'accroissement de l'efficacité et d'économies d'échelle. Elle permet également d'éviter la multiplication des infrastructures administratives et de réduire les dépenses administratives improductives, tout en garantissant un niveau élevé de gestion des services publics.

En 2008, 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 de niveau de service qui ont été signés depuis le début avec les diverses institutions et leurs services sont régulièrement mis à jour. En septembre 2008, le CEPD a signé un nouvel accord de niveau de service avec le service médical de la Commission.

En outre, il a signé une délégation de pouvoir en faveur du PMO pour les activités quotidiennes liées à la gestion des droits de pension. Des accords couvrant de nouveaux domaines sont en cours de préparation.

Le CEPD a obtenu un accès direct à certaines applications de gestion financière de la Commission, dans le but de faciliter la coopération entre les services de la Commission et le CEPD et d'améliorer l'échange d'informations entre les services.

La nouvelle version du site Internet du CEPD, réalisée en coopération avec les services compétents du Parlement européen, a été achevée en 2008. Toutefois, certains problèmes liés au logiciel qui avait été spécifiquement choisi pour cette tâche ont ralenti la mise en service de nouvelles fonctions web déjà développées. Le CEPD compte terminer ce projet au cours de l'année 2009.

La participation à l'appel d'offres interinstitutionnel pour les formations générales et linguistiques, les

assurances et le mobilier s'est poursuivie en 2008, 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 européen.

Le CEPD a continué à participer aux travaux de divers comités interinstitutionnels. Cette participation est particulièrement active au sein du *Comité de gestion assurances maladies* (CGAM), du *Comité de préparation pour les questions statutaires* (CPQS) et du *Comité du Statut*, pour lesquels le CEPD est représenté dans différents groupes de travail. Cependant, en raison de la taille réduite de l'institution, elle a dû être limitée à certains comités seulement. 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.

### 6.6.2. 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 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.

Cinq décisions internes importantes ont été adoptées en 2008 :

- Règles du 16 juin 2008 relatives au remboursement des frais exposés par les personnes extérieures aux services du CEPD invitées à participer à des réunions en qualité d'expert ;
- Décision du 8 août 2008 de l'ordonnateur délégué relative à l'archivage des documents financiers et des pièces justificatives ;
- Décision du 2 octobre 2008 du Contrôleur concernant les modalités d'application générale de l'article 45 bis du Statut (certification) ;

- Décision du 16 décembre 2008 du Contrôleur portant adoption de mesures de sécurité au sein du CEPD ;
- Décision du 19 décembre 2008 du Contrôleur portant nomination d'un responsable local de la sécurité au sein du CEPD.

Le CEPD est une institution relativement nouvelle qui connaît une évolution rapide. En conséquence, les règles et procédures qui étaient adaptées au aux premières années d'activité pourront s'avérer moins efficaces à l'avenir, dans le cadre d'une structure plus importante et plus complexe. C'est pourquoi les règles existantes feront l'objet d'une évaluation qui sera effectuée deux ans après leur adoption, et pourraient donc être modifiées en conséquence.

### 6.6.3. Gestion des documents

La mise en œuvre d'un nouveau système de gestion du courrier électronique (GEDA) s'est poursuivie, malgré quelques retards dus à des difficultés imprévues. Le processus devrait être achevé en 2009, avec l'aide des services du Parlement européen. Cette mise en œuvre est conçue comme la première étape de la mise en place d'un système de gestion des dossiers destiné à mieux soutenir les activités du CEPD.

## 6.7. Objectifs pour 2009

Les objectifs fixés pour 2008 ont été atteints. En 2009, le CEPD poursuivra le processus de consolidation engagé auparavant et développera davantage certaines activités.

Le CEPD poursuivra l'adoption de nouvelles règles financières internes adaptées à la taille de l'institution. Pour ce qui est des logiciels financiers, il poursuivra les efforts déployés pour acquérir les outils permettant d'accéder 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. Celui-ci a l'intention de signer un accord de coopération avec la Commission (Adminfo) afin de faciliter l'intégration et l'installation des nouveaux collègues. Parallèlement, il continuera à développer l'environnement administratif de ses services et à adopter des dispositions générales d'application du Statut.

Le CEPD envisage d'organiser, avec l'aide de l'Office européen de sélection du personnel (EPSO), un concours général dans le domaine de la protection des données, afin de recruter du personnel hautement spécialisé.

Pour ce qui est des logiciels de gestion des ressources humaines (principalement missions : MIP ; vacances et formations : Syslog), le CEPD entreprendra également les démarches nécessaires pour acquérir les programmes permettant d'accéder aux dossiers depuis ses locaux.

Le CEPD prévoit de procéder à une évaluation complète des risques dans le but de déterminer si les normes internes existantes en matière de contrôle sont adaptées au regard des pratiques actuelles de l'institution.

La mise en œuvre des améliorations recensées au cours de l'évaluation du système de contrôle interne, ainsi que la mise en œuvre des recommandations du Service d'audit interne, resteront des priorités importantes.

Le DPD continuera à assurer l'application interne des dispositions du règlement (CE) n° 45/2001. Un registre des notifications sera mis en place.

Des espaces de bureaux supplémentaires seront nécessaires pour accueillir le personnel futur. Des négociations en vue d'obtenir suffisamment d'espace pour couvrir les besoins futurs seront engagées avec les services du Parlement européen au cours de 2009.

Le CEPD a l'intention d'achever, avec l'aide du Parlement européen, la mise en œuvre du système de gestion du courrier électronique et de mettre la dernière main au développement du nouveau site web.



## 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 des 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, une directive particulière qui a 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 qui a commencé 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 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 à ce jour été ratifiée par plus de 40 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, pour 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>(70)</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 et soumis à la ratification de tous les États membres, 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 aux 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 comme une question horizontale à l'article 16 du traité sur le fonctionnement de l'UE. Il est ainsi manifeste que la protection des données est 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 regardant 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.

<sup>(70)</sup> JO L 8 du 12.1.2001, p. 1.

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 européen. Il traite ainsi 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 obligations 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 un délégué à la protection des données (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 la plupart des 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 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 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 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 réclamations, effectuer d'autres 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 contrôle 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 d'autres mesures destinées à s'appliquer au niveau national ou à être transposées en droit 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 et intervenir dans les affaires portées devant la Cour de justice constituent d'autres tâches importantes. 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 avec les organes de contrôle relevant du troisième pilier a une incidence similaire. En tant que membre du Groupe article 29 sur la protection des données, qui a été institué pour conseiller la Commission européenne et pour développer des politiques harmonisées, le CEPD a la possibilité de contribuer aux travaux menés à ce niveau. 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 au 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 pour 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 pour 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) 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 ;  
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), à l'article 10, 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

ACC	Autorité de contrôle commune
ACCP	Agence communautaire de contrôle des pêches
AEM	Agence européenne des médicaments
AESM	Agence européenne pour la sécurité maritime
ARES	Système avancé d'enregistrement
BCE	Banque centrale européenne
BEI	Banque européenne d'investissement
CC	Cour des comptes
CCR	Centre commun de recherche
CCTV	Télévision en circuit fermé]
CdR	Comité des régions
CdT	Centre de traduction des organes de l'Union européenne
CE	Communautés européennes
Cedefop	Centre européen pour le développement de la formation professionnelle
CEDH	Convention européenne des droits de l'homme
CESE	Comité économique et social européen
CIG	Conférence intergouvernementale
CJCE	Cour de justice des Communautés européennes.
CMT	Centre de médecine du travail
CPD	Coordinateur de la protection des données (à la Commission européenne uniquement)
DG ADMIN	Direction générale Personnel et administration
DG EAC	Direction générale Éducation et culture
DG EMPL	Direction générale Emploi, affaires sociales et égalité des chances
DG INFO	Direction générale Société de l'information et médias
DG JLS	Direction générale Justice, liberté et sécurité
DIGIT	Direction générale Informatique
DPA	Autorité chargée de la protection des données
DPD	Délégué à la protection des données
ECRIS	Système européen d'information sur les casiers judiciaires
EEA	École européenne d'administration
EFSA	Autorité européenne de sécurité des aliments
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
EPSO	Office européen de sélection du personnel
EUMC	Observatoire européen des phénomènes racistes et xénophobes
Eurofound	Fondation européenne pour l'amélioration des conditions de vie et de travail
FEF	Fondation européenne pour la formation
FIDE	Fichier d'identification des dossiers d'enquêtes douanières
FRA	Agence des droits fondamentaux de l'Union européenne

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
NSA	Agence de sécurité nationale
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
OLAF	Office européen de lutte antifraude
PMO	Office payeur de la Commission européenne
PNR	Dossier passager
PPE	Personne politiquement exposée
R & D	Recherche et développement
Radio-identification (RFID)	Identification par radiofréquence
SAI	Service d'audit interne
SAR	Système d'alerte rapide
SCPC	Système de coopération en matière de protection des consommateurs
SGI	Service de gestion de l'identité
SID	Système d'information douanier
SIR	Système informatisé de réservation
SIS	Système d'information Schengen
SWIFT	Société de télécommunications interbancaires mondiales
UE	Union européenne
VIS	Système d'information sur les visas
WP 29	Groupe de l'article 29

## Annexe D

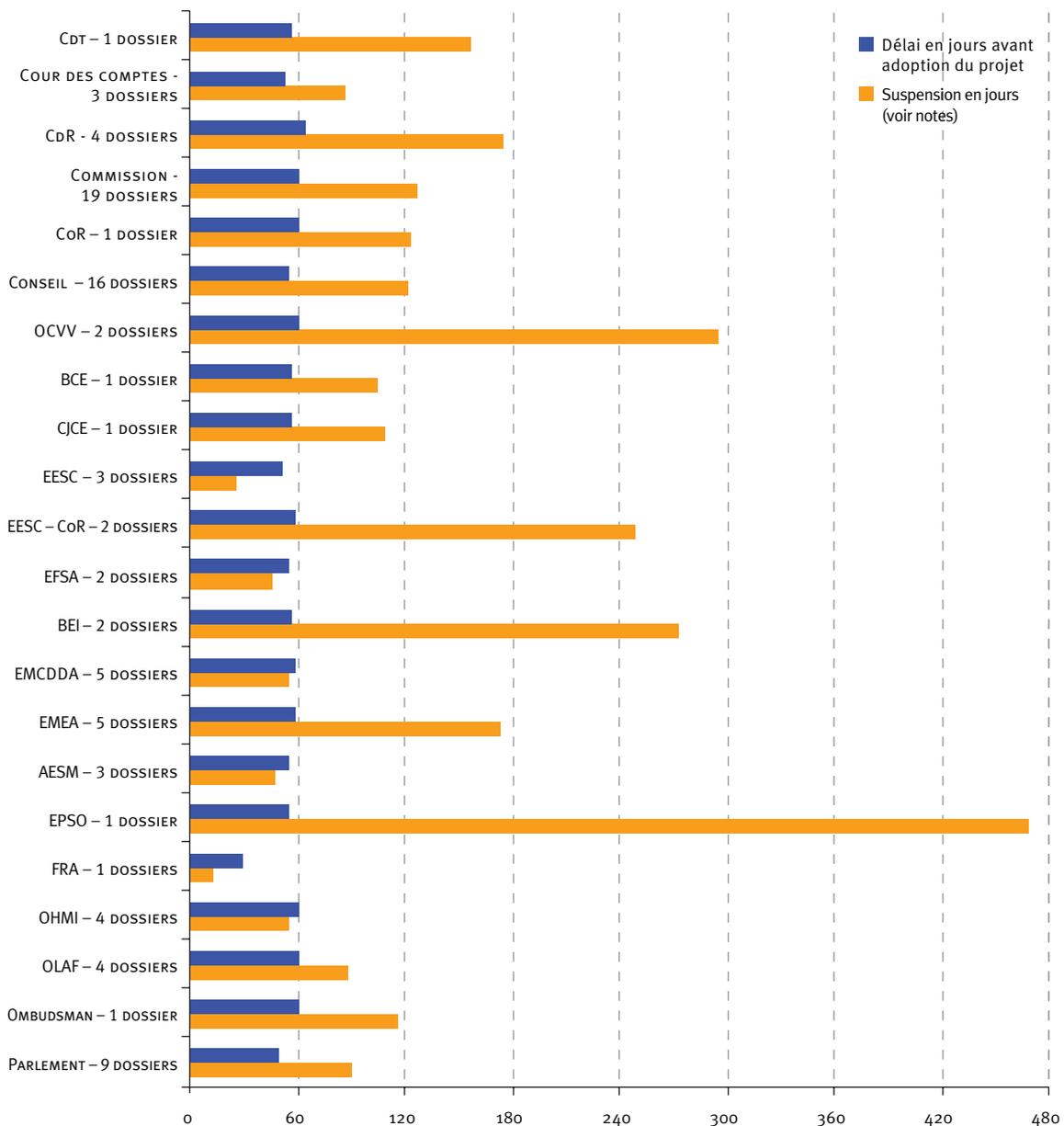
## Liste des délégués à la protection des données (DPD)

Organisation	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	Maria ARSENE	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
Médiateur européen	Loïc JULIEN	dpo-euro-ombudsman@ombudsman.europa.eu
Contrôleur européen de la protection des données	Giuseppina LAURITANO	giuseppina.lauritano@edps.europa.eu
Banque centrale européenne	Martin BENISCH	DPO@ecb.int
Office européen de lutte antifraude (OLAF)	Laraine LAUDATI	laraine.laudati@ec.europa.eu
Centre de traduction des organes de l'Union européenne	Benoît VITALE	data-protection@cdt.europa.eu
Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles) (OHMI)	Ignacio DE MEDRANO CABALLERO	dataprotectionofficer@oami.europa.eu
Agence des droits fondamentaux de l'Union européenne (FRA)	Nikolaos FIKATAS	nikolaos.fikatas@fra.europa.eu
Agence européenne des médicaments (EMA)	Vincenzo SALVATORE	data.protection@emea.europa.eu
Office communautaire des variétés végétales (OCVV)	Véronique DOREAU	doreau@cpvo.europa.eu
Fondation européenne pour la formation (FEF)	Liia KAARLOP	liia.kaarlop@etf.europa.eu
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)	Andreas MITRAKAS	dataprotection@enisa.europa.eu
Fondation européenne pour l'amélioration des conditions de vie et de travail (Eurofound)	Markus GRIMMEISEN	mgr@eurofound.europa.eu
Observatoire européen des drogues et des toxicomanies (OEDT)	Cécile MARTEL	cecile.martel@emcdda.europa.eu
Autorité européenne de sécurité des aliments (EFSA)	Claus REUNIS	dataprotectionofficer@efsa.europa.eu
Agence européenne pour la sécurité maritime (AESM)	Malgorzata NESTEROWICZ	malgorzata.nesterowicz@emsa.europa.eu
Agence européenne pour la reconstruction (AER)	Richard LUNDGREN	richard.lundgren@ear.europa.eu
Centre européen pour le développement de la formation professionnelle (Cedefop)	Spyros ANTONIOU	spyros.antoniou@cedefop.europa.eu
Agence exécutive « Éducation, audiovisuel et culture » (EACEA)	Hubert MONET	hubert.monet@ec.europa.eu

Organisation	Nom	Adresse électronique
Agence européenne pour la sécurité et la santé au travail (OSHA)	Terry TAYLOR	taylor@osha.europa.eu
Agence communautaire de contrôle des pêches (ACCP)	Rieke ARNDT	rieko.arndt@cfca.europa.eu
Autorité de surveillance du GNSS européen	Christina TSALI	christina.tsali@gsa.europa.eu
Agence ferroviaire européenne (ERA)	Zographia PYLORIDOU	zographia.pyloridou@era.europa.eu
Agence exécutive pour le programme de santé publique	Eva LÄTTI	eva.latti@ec.europa.eu
Centre européen pour la prévention et le contrôle des maladies (ECDC)	Elisabeth ROBINO	elisabeth.robino@ecdc.europa.eu
Agence européenne pour l'environnement (AEE)	Gordon McINNES	gordon.mcinnes@eea.europa.eu
Fonds européen d'investissement (FEI)	Jobst NEUSS	j.neuss@eif.org
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
Agence exécutive pour la compétitivité et l'innovation (EACI)	Elena FIERRO SEDANO	elena.ferro-sedano@ec.europa.eu
Agence exécutive du réseau transeuropéen de transport (AE RTE-T)	Elisa DALLE MOLLE	Elisa.dalle-molle@ext.ec.europa.eu
Agence européenne des produits chimiques (ECHA)	Minna HEIKKILA	minna.heikkila@echa.europa.eu

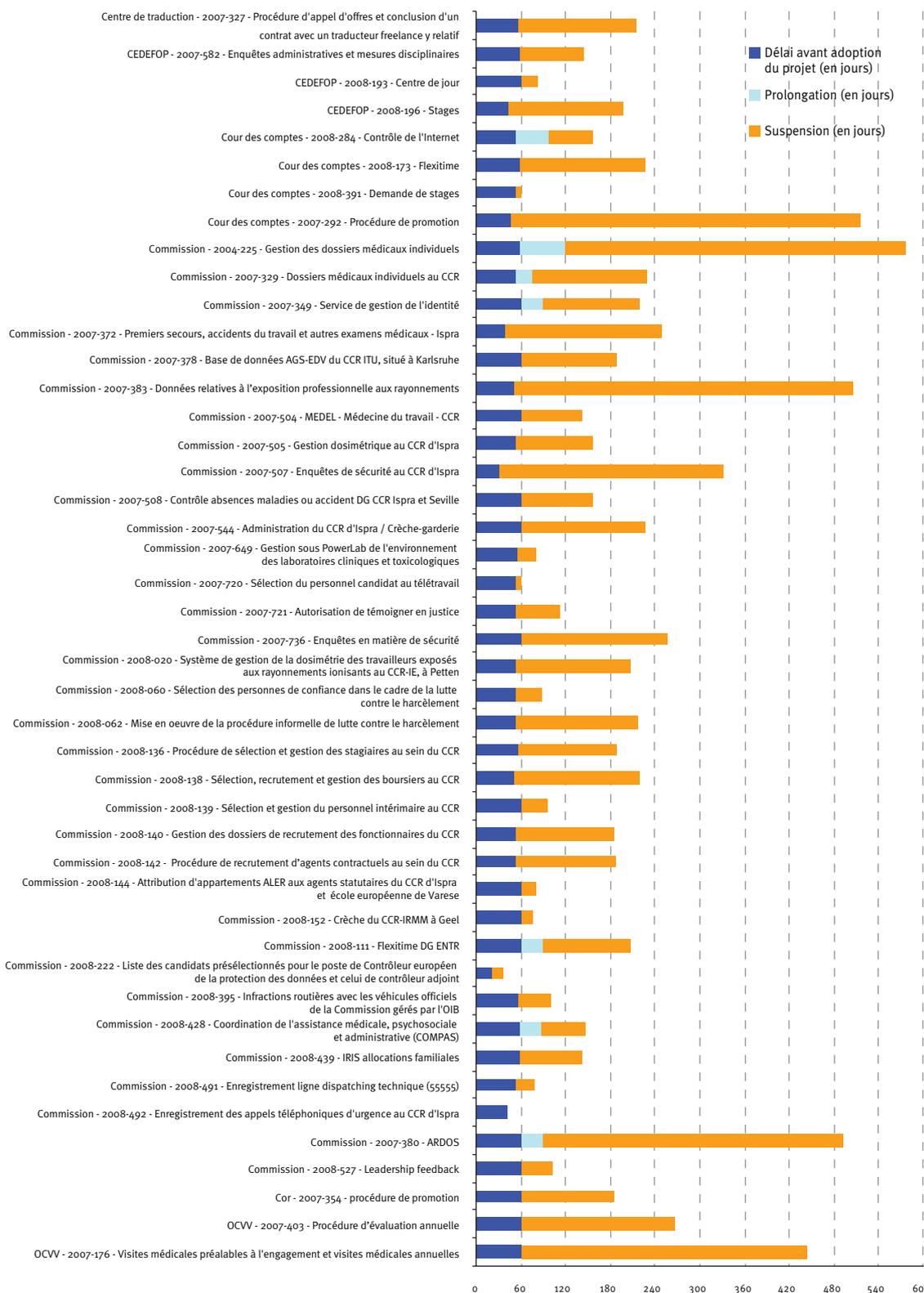
Annexe E

## Délais de traitement des contrôles préalables par dossier et par institution

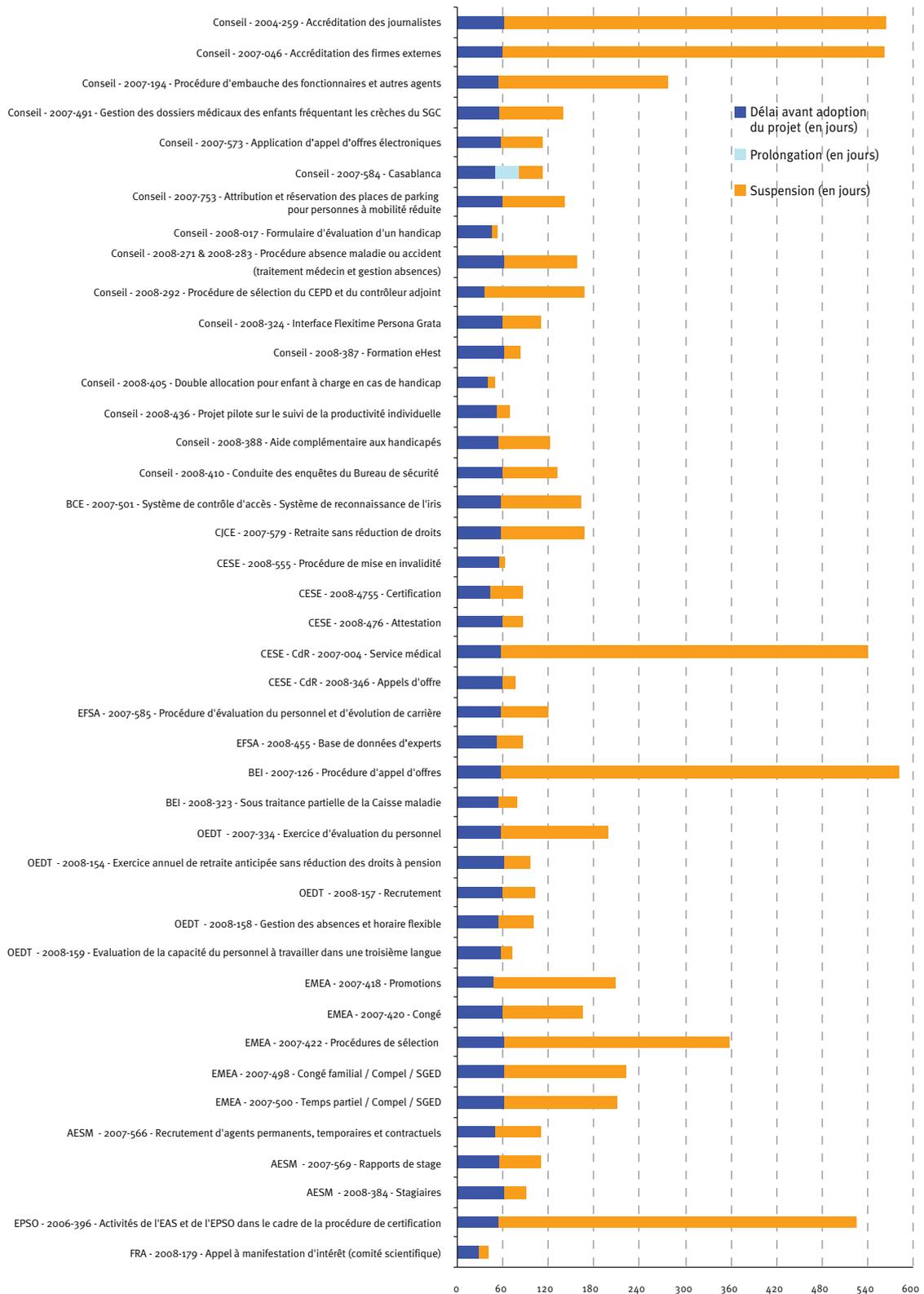


NB: Le mois d'août n'est pas inclus dans les jours pris pour l'élaboration des projets d'avis concernant les dossiers a posteriori reçus avant le 1<sup>er</sup> septembre 2008. Les jours de suspension incluent la suspension accordée pour les éventuels commentaires sur le projet d'avis, normalement de 7 à 10 jours.

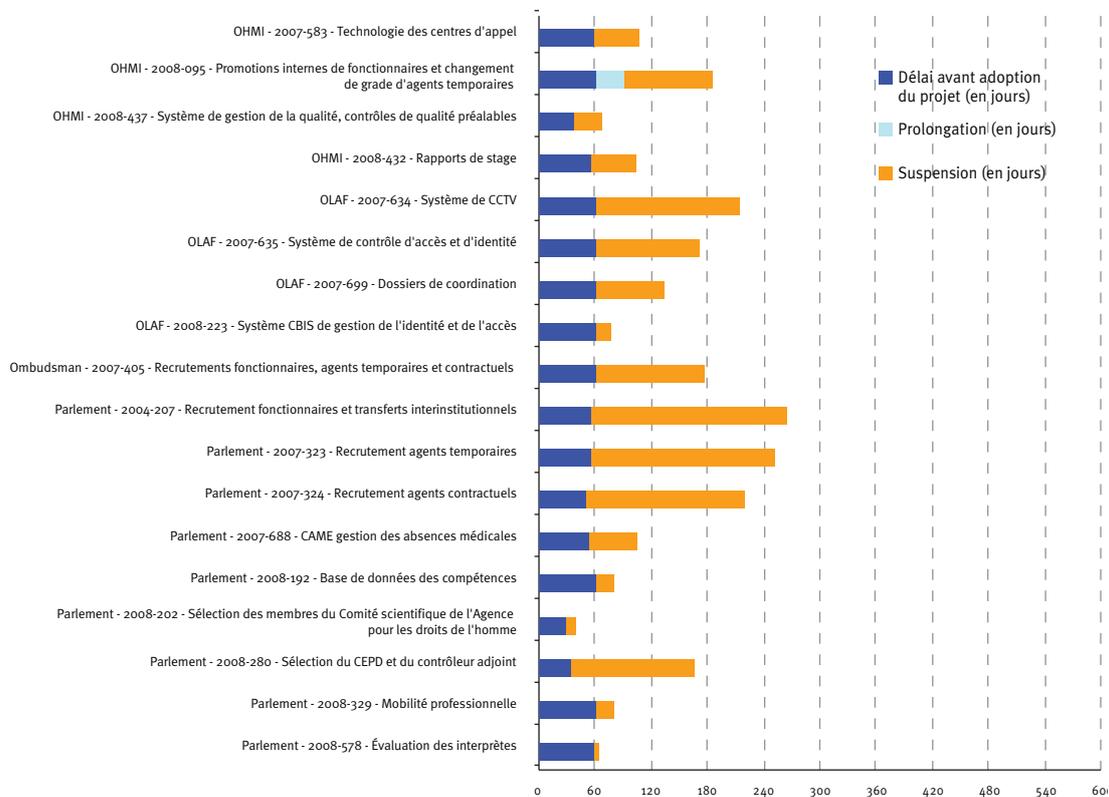
**Avis rendus en 2008 (I)**



**Avis rendus en 2008 (2)**



**Avis rendus en 2008 (3)**



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 2008. Les jours de suspension incluent la suspension accordée pour les éventuels commentaires sur le projet d'avis, normalement de 7 à 10 jours.

## Annexe F

## Liste des avis rendus à la suite d'un contrôle préalable

### Base de données ARDOS — Commission

Avis du 15 décembre 2008 sur une notification en vue d'un contrôle préalable concernant la base de données ARDOS (Dossier 2007-380)

### « Leadership feedback » — Commission

Avis du 15 décembre 2008 sur la notification en vue d'un contrôle préalable à propos de la procédure facultative de « Leadership Feedback » mise en place par l'École européenne d'administration (EAS) en rapport avec ses cours de management (Dossier 2008 527)

### Enquêtes du Bureau de sécurité — Conseil

Avis du 12 décembre 2008 sur la notification à propos de la conduite des enquêtes du Bureau de sécurité (Dossier 2008 410)

### Appels d'offres — Banque européenne d'investissement

Avis du 5 décembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Appels d'offres » (Dossier 2007-126)

### Évaluation des interprètes — Parlement

Avis du 5 décembre 2008 sur une notification en vue d'un contrôle préalable concernant le dossier « Évaluation des interprètes » (Dossier 2008-578)

### Recrutement de stagiaires — Cedefop

Avis du 5 décembre 2008 sur une notification en vue d'un contrôle préalable concernant le recrutement de stagiaires (Dossier 2008-196)

### Flexitime — Cour des comptes

Avis du 5 décembre 2008 sur la notification d'un contrôle préalable à propos du traitement des données « Système de gestion et de contrôle du Flexitime » (Dossier 2008-173)

### IRIS : allocations familiales — Commission

Avis du 5 décembre 2008 sur la notification d'un contrôle préalable à propos du dossier « IRIS : allocations familiales » (Dossier 2008-439)

### COMPAS — Commission

Avis du 4 décembre 2008 sur une notification en vue d'un contrôle préalable concernant la « Coordination de l'assistance médicale, psychosociale et administrative (COMPAS) » (Dossier 2008 428)

### Certification — Comité économique et social

Avis du 26 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Procédure de certification » (Dossier 2008-475)

### Aide complémentaire aux handicapés — Conseil

Avis du 25 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Aide complémentaire aux handicapés » (Dossier 2008-388)

**Rapports de stage — OHMI**

Avis du 25 novembre 2008 sur une notification en vue d'un contrôle préalable concernant les rapports de stage (Dossier 2008-432)

**Attestation — Comité économique et social**

Avis du 25 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « procédure d'attestation » (Dossier 2008-476)

**Promotion — Cour des comptes**

Avis du 24 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « procédure de promotion » (Dossier 2007-292)

**Enregistrement des appels au dispatching technique — Commission**

Avis du 19 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles » (Dossier 2008-491)

**Mise en invalidité — Comité économique et social**

Avis du 19 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Procédure de mise en invalidité » (Dossier 2008-555)

**Dossiers médicaux individuels — Commission**

Avis du 18 novembre 2008 sur la notification d'un contrôle préalable à propos de la « gestion des dossiers médicaux individuels Bruxelles — Luxembourg » (Dossier 2004-225)

**Recrutement de directeurs — OHMI**

Avis du 12 novembre 2008 sur une notification en vue d'un contrôle préalable concernant le recrutement de directeurs (Dossier 2008-435)

**Absence pour maladie ou accident — Conseil**

Avis du 11 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Procédure en cas d'absence pour maladie ou accident » (Dossiers 2008-271 et 2008-283)

**Base de données d'experts — Autorité européenne de sécurité des aliments**

Avis du 11 novembre 2008 sur la notification d'un contrôle préalable à propos de la base de données d'experts de l'Autorité européenne de sécurité des aliments (Dossier 2008-455)

**Contrôle de l'Internet — Cour des comptes**

Avis du 10 novembre 2008 sur la notification d'un contrôle préalable concernant le contrôle de l'Internet (Dossier 2008-284)

**Promotion des fonctionnaires et reclassement des agents temporaires — OHMI**

Avis du 7 novembre 2008 sur une notification en vue d'un contrôle préalable à propos du dossier « Promotion interne des fonctionnaires et reclassement des agents temporaires » (Dossier 2008-95)

**Exposition aux rayonnements — Commission**

Avis du 5 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Données relatives à l'exposition professionnelle aux rayonnements » (Dossier 2007-385)

**Infractions routières — Commission**

Avis du 3 novembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Infractions routières avec les véhicules officiels de la Commission gérés par l'Office Infrastructures et Logistique de Bruxelles (OIB) » (Dossier 2008-395)

**Formation eHEST — Conseil**

Avis du 22 octobre 2008 sur une notification en vue d'un contrôle préalable concernant la formation eHEST (Computer based Hostile Environment Security Training) (Dossier 2008-387)

**Contrôles de qualité — OHMI**

Avis du 22 octobre 2008 sur une notification en vue d'un contrôle préalable concernant les contrôles de qualité (Dossier 2008-437)

**Sélection du CEPD et du Contrôleur adjoint — Parlement européen et Conseil**

Avis du 21 octobre 2008 sur la notification de contrôle préalable concernant la sélection du Contrôleur européen de la protection des données et du Contrôleur européen de la protection des données adjoint (Dossiers 2008-280 et 2008-292)

**Enregistrement des appels d'urgence sur le site du CCR d'Ispra — Commission**

Lettre du 13 octobre 2008 en réponse à la notification en vue d'un contrôle préalable concernant l'enregistrement des appels d'urgence sur le site du CCR d'Ispra (Dossier 2008-492)

**Boursiers au Centre commun de recherche (CCR) — Commission**

Avis du 9 octobre 2008 sur une notification en vue d'un contrôle préalable concernant la sélection, le recrutement et la gestion des boursiers au Centre commun de recherche (CCR) (Dossier 2008-138)

**Stagiaires au Centre commun de recherche (CCR) — Commission**

Avis du 9 octobre 2008 sur une notification en vue d'un contrôle préalable concernant la procédure de sélection et la gestion des stagiaires au sein du Centre commun de recherche (CCR) (Dossier 2008-136)

**Procédure de recrutement d'agents contractuels au CCR — Commission**

Avis du 9 octobre 2008 sur une notification en vue d'un contrôle préalable concernant la procédure de recrutement d'agents contractuels au sein du Centre commun de recherche (CCR) (Dossier 2008-142)

**Dossiers de recrutement des fonctionnaires du CCR — Commission**

Avis du 9 octobre 2008 sur la notification d'un contrôle préalable concernant la gestion des dossiers de recrutement des fonctionnaires du CCR (transferts et lauréats de concours généraux) (Dossier 2008-140)

**Enquêtes en matière de sécurité — Commission**

Avis du 2 octobre 2008 sur une notification de contrôle préalable à propos des enquêtes en matière de sécurité (Dossier 2007-736)

**Projet pilote sur le suivi de la productivité individuelle — Conseil**

Avis du 1<sup>er</sup> octobre 2008 sur la notification de contrôle préalable au sujet d'un projet pilote sur le suivi de la productivité individuelle : traitement ultérieur des données à caractère personnel dans l'application Workflow (Dossier 2008-436)

**Réseau de personnes de confiance (harcèlement) — Commission**

Avis du 30 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier « mise en œuvre par le service gestionnaire et le réseau des personnes de confiance de la procédure informelle de lutte contre le harcèlement moral et le harcèlement sexuel à la Commission européenne (procédure contre le harcèlement) » (Dossier 2008-62)

**Recrutement de stagiaires — EMSA**

Avis du 29 septembre 2008 concernant une notification relative à un contrôle préalable à propos du dossier « Recrutement de stagiaires dans le cadre du programme de stages de l'EMSA » (Dossier 2008-384)

**Double allocation pour enfant à charge — Conseil**

Avis du 29 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Double allocation pour enfant à charge en cas de handicap » (Dossier 2008-405)

**Stage — Cour des comptes**

Avis du 19 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier « demandes de stage rémunéré ou non-rémunéré » (Dossier 2008-391)

### **Mobilité professionnelle — Parlement**

Avis du 17 septembre 2008 sur la notification d'un contrôle préalable concernant le traitement « mobilité professionnelle » (Dossier 2008-329)

### **Sous-traitance de la caisse de maladie — BEI**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier « sous-traitance partielle de la caisse de maladie » (Dossier 2008-323)

### **Accréditation des journalistes — Conseil**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable sur l'accréditation de journalistes participant aux réunions du Conseil européen (Dossier 2004-259)

### **Accréditation du personnel des firmes externes — Conseil**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable sur l'accréditation du personnel des firmes externes participant aux réunions du Conseil européen (Dossier 2007-46)

### **Interface Flexitime/PersonaGrata — Conseil**

Avis du 16 septembre 2008 sur la notification d'un contrôle préalable à propos du dossier « Interface Flexitime — PersonaGrata (DGA3) » (Dossier 2008-324)

### **Appels d'offres et contrats — CdR et CESE**

Avis du 15 septembre 2008 sur une notification en vue d'un contrôle préalable concernant les traitements de données pour gérer les appels d'offres et les contrats (Dossier 2008-346)

### **Interface Flexitime TIM à la DG Entreprises et industrie — Commission**

Réponse du 15 septembre 2008 à une notification en vue d'un contrôle préalable concernant l'interface Flexitime TIM à la DG Entreprises et industrie (Dossier 2008-111)

### **Système de gestion de la dosimétrie — Commission**

Avis du 3 septembre 2008 sur la notification d'un contrôle préalable concernant le système de gestion de la dosimétrie des travailleurs exposés aux rayonnements ionisants au CCR-IE, à Petten (Dossier 2008-20)

### **Enquêtes de sécurité au CCR d'Ispra — Commission**

Avis du 31 juillet 2008 sur une notification de contrôle préalable à propos des enquêtes de sécurité au Centre commun de recherche d'Ispra (Dossier 2007-507)

### **Service conjoint médico-social — CdR et CESE**

Avis du 4 juillet 2008 sur la notification d'un contrôle préalable à propos du dossier « service conjoint médico-social » (Dossier 2007-004)

### **Système de gestion de l'identité et de l'accès — OLAF**

Avis du 30 juin 2008 sur une notification en vue d'un contrôle préalable relative au système CBIS de gestion de l'identité et de l'accès (Dossier 2008-223)

### **Centre de jour — Cedefop**

Avis du 20 juin 2008 sur une notification en vue d'un contrôle préalable concernant le « Centre de jour » (Dossier 2008-193)

### **Recrutement — Observatoire européen des drogues et des toxicomanies (OEDT)**

Avis du 20 juin 2008 sur une notification en vue d'un contrôle préalable relative au recrutement du personnel (Dossier 2008-157)

### **Absences et flexitime — OEDT**

Avis du 20 juin 2008 sur une notification de contrôle préalable au sujet de la gestion des absences et de l'horaire flexible (Dossier 2008-158)

**Recrutement — Agence européenne des médicaments**

Avis du 19 juin 2008 sur la notification d'un contrôle préalable concernant la base de données de recrutement « Access » et les procédures de sélection et de recrutement de l'EMA (Dossier 2007-422)

**Retraite anticipée — OEDT**

Avis du 16 juin 2008 sur la notification d'un contrôle préalable à propos du dossier « Exercice annuel de retraite anticipée sans réduction des droits à pension » (Dossier 2008-154)

**Base de données SKILLS — Parlement**

Avis du 13 juin 2008 sur la notification en vue d'un contrôle préalable à propos de la base de données SKILLS (Dossier 2008-192)

**Sélection et gestion du personnel intérimaire au CCR — Commission**

Avis du 9 juin 2008 sur la notification d'un contrôle préalable concernant la sélection et la gestion du personnel intérimaire au Centre commun de recherche (CCR) (Dossier 2008-139)

**Visites médicales — OCVV**

Avis du 4 juin 2008 sur la notification en vue d'un contrôle préalable concernant les visites médicales préalables à l'engagement et les visites médicales annuelles à l'OCVV (Dossier 2007-176)

**Parking pour les personnes à mobilité réduite — Conseil**

Avis du 29 mai 2008 sur la notification d'un contrôle préalable à propos du dossier de l'attribution et la réservation de places de parking aux personnes à mobilité réduite (PMR) (Dossier 2007-753)

**Attribution d'appartements de l'ALER — Commission**

Avis du 26 mai 2008 sur une notification en vue d'un contrôle préalable concernant l'attribution d'appartements de l'ALER au personnel statutaire du CCR d'Ispra et de l'école européenne à Varese (Dossier 2008-144)

**Crèche du CCR-IRMM à Geel — Commission**

Avis du 23 mai 2008 sur une notification en vue d'un contrôle préalable concernant le traitement des données à caractère personnel de la crèche du CCR-IRMM à Geel (Dossier 2008-152)

**Troisième langue — OEDT**

Avis du 20 mai 2008 sur la notification d'un contrôle préalable concernant l'évaluation de la capacité du personnel à travailler dans une troisième langue (Dossier 2008-159)

**Système de CCTV — OLAF**

Avis du 19 mai 2008 sur la notification de contrôle préalable concernant le système de télévision en circuit fermé (système de CCTV) de l'OLAF (Dossier 2007-634)

**Candidats présélectionnés pour le poste de Contrôleur européen de la protection des données et le poste de Contrôleur adjoint — Commission**

Avis du 16 mai 2008 sur la notification d'un contrôle préalable en vue d'établir une liste de candidats présélectionnés pour le poste de Contrôleur européen de la protection des données et le poste de Contrôleur adjoint (Dossier 2008-222)

**Procédure de sélection des membres du Comité scientifique — Agence pour les droits de l'homme**

Avis du 29 avril 2008 sur une notification en vue d'un contrôle préalable concernant la procédure de sélection des membres du Comité scientifique (Dossiers joints 2008-179 et 2008-202)

**Personnes de confiance dans le cadre du harcèlement — Commission**

Avis du 29 avril 2008 sur la notification de contrôle préalable à propos du dossier « Sélection des personnes de confiance dans le cadre de la lutte contre le harcèlement moral et le harcèlement sexuel à la Commission européenne » (Dossier 2008-60)

**Lieux d'accueil pour enfants du CCR à Ispra — Commission**

Avis du 21 avril 2008 sur une notification en vue d'un contrôle préalable concernant la gestion des lieux d'accueil pour enfants (Crèche/Garderie) du CCR à Ispra (Dossier 2007-544)

**Congé familial — EMEA**

Avis du 14 avril 2008 sur la notification d'un contrôle préalable à propos du dossier « congé familial/base de données Compel sur le personnel/systèmes de gestion électronique des documents (SGED) » (Dossier 2007-498)

**Procédure d'évaluation annuelle — OCVV**

Avis du 14 avril 2008 sur la notification d'un contrôle préalable concernant la procédure d'évaluation annuelle (Dossier 2007-403)

**Système de contrôle d'accès et d'identité — OLAF**

Avis du 7 avril 2008 sur la notification d'un contrôle préalable concernant un système de contrôle d'accès et d'identité (Dossier 2007-635)

**Dossiers de coordination — OLAF**

Avis du 7 avril 2008 sur la notification de contrôle préalable concernant les dossiers relatifs aux opérations de coordination (dossiers de coordination) (Dossier 2007-699)

**Demandes de temps partiel — Agence européenne des médicaments**

Avis du 1er avril 2008 sur la notification d'un contrôle préalable à propos des demandes d'exercice de l'activité de temps partiel (Dossier 2007-500)

**Autorisations de témoigner en justice — Commission**

Avis du 28 mars 2008 sur la notification d'un contrôle préalable à propos du dossier « Autorisations de témoigner en justice » (Dossier 2007-721)

**Départ à la retraite sans réduction des droits — Cour de justice**

Avis du 17 mars 2008 sur la notification de contrôle préalable à propos du dossier « départ à la retraite sans réduction des droits à pension » (Dossier 2007-579)

**Recrutement des fonctionnaires et transferts interinstitutionnels — Parlement**

Avis du 13 mars 2008 sur la notification d'un contrôle préalable à propos du dossier « recrutement des fonctionnaires et transferts interinstitutionnels » (Dossier 2004-207)

**Recrutement des agents temporaires — Parlement**

Avis du 13 mars 2008 sur la notification d'un contrôle préalable à propos du dossier « recrutement des agents temporaires » (Dossier 2007-323)

**Recrutement des agents contractuels — Parlement**

Avis du 13 mars 2008 sur la notification d'un contrôle préalable à propos du dossier « recrutement des agents contractuels » (Dossier 2007-384)

**Evaluation d'un handicap — Conseil**

Avis du 7 mars 2008 sur la notification d'un contrôle préalable à propos du dossier « formulaire d'évaluation d'un handicap » (Dossier 2008-17)

**Activités de l'École européenne d'administration et d'EPSO dans le cadre de la certification — Commission**

Avis du 7 mars 2008 sur la notification d'un contrôle préalable à propos du dossier « Activités de l'École européenne d'administration et d'EPSO dans le cadre de la procédure de certification » (Dossier 2006-396)

**Gestion des absences médicales — Parlement**

Avis du 4 mars 2008 sur la notification d'un contrôle préalable à propos du dossier « CAME — gestion des absences médicales » (Dossier 2007-688)

**Promotion des agents temporaires — EMEA**

Avis du 20 février 2008 sur la notification d'un contrôle préalable sur la promotion des agents temporaires (Dossier 2007-418)

**Système de contrôle par analyse de l'iris — Banque centrale européenne**

Avis du 14 février 2008 rendu à la suite d'une notification concernant l'intégration dans un système de contrôle d'accès préexistant d'une technologie d'analyse de l'iris pour les zones hautement sécurisées de la BCE (Dossier 2007-501)

**Enquêtes administratives et procédures disciplinaires — Cedefop**

Avis du 13 février 2008 sur une notification en vue d'un contrôle préalable concernant le traitement de données dans le cadre d'enquêtes administratives et de procédures disciplinaires (Dossier 2007-582)

**Contrôle des absences au CCR à Ispra et à Séville — Commission**

Avis du 6 février 2008 sur la notification d'un contrôle préalable à propos du dossier « Contrôle des absences du travail pour maladie ou accident – DG CCR Ispra et Séville » (Dossier 2007-508)

**Système de gestion de la dosimétrie — Commission**

Avis du 6 février 2008 sur une notification de contrôle préalable à propos du dossier « Système de gestion dosimétrique au Centre commun de recherche d'Ispra » (Dossier 2007-505)

**Service de gestion de l'identité — Commission**

Avis du 6 février 2008 sur une notification en vue d'un contrôle préalable concernant le service de gestion de l'identité (Dossier 2007-349)

**Candidats au télétravail — Commission**

Avis du 6 février 2008 sur la notification de contrôle préalable à propos du dossier « Sélection du personnel candidat au télétravail » (Dossier 2007-720)

**Dossiers médicaux individuels au CCR — Commission**

Avis du 6 février 2008 sur une notification de contrôle préalable concernant le traitement des dossiers médicaux individuels au Centre commun de recherche à Ispra et à Séville (Dossier 2007-329)

**Évaluation du personnel et évolution de carrière — EFSA**

Avis du 25 janvier 2008 sur une notification de contrôle préalable concernant la procédure d'évaluation du personnel et d'évolution de carrière (Dossier 2007-585)

**CASABLANCA — Conseil**

Avis du 25 janvier 2008 sur la notification de contrôle préalable à propos du dossier « CASABLANCA (gestion des actions de formation professionnelle) » (Dossier 2007-584)

**Examens médicaux au CCR à Ispra — Commission**

Avis du 25 janvier 2008 concernant « les premiers soins, les accidents du travail et autres examens médicaux » au CCR (Centre commun de recherche) à Ispra (Dossier 2007-372)

**Procédure d'embauche — Conseil**

Avis du 25 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier « Procédure d'embauche des fonctionnaires et autres agents du Secrétariat général du Conseil » (Dossier 2007-194)

**Médecine du travail — Commission**

Avis du 23 janvier 2008 concernant une notification relative à un contrôle préalable concernant la médecine du travail (MeDel) au sein de la Direction générale Centre commun de recherche (Dossier 2007-504)

**Gestion sous PowerLab — Commission**

Avis du 17 janvier 2008 concernant une notification en vue d'un contrôle préalable concernant la « gestion sous PowerLab de l'environnement des laboratoires cliniques et toxicologiques » (Dossier 2007-649)

**Contrat de traducteur freelance — Centre de traduction**

Avis du 17 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier « appel d'offre et passation d'un contrat avec un traducteur freelance » (Dossier 2007-327)

**Dossiers médicaux des enfants de la crèche — Conseil**

Avis du 17 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier « Gestion des dossiers médicaux des enfants fréquentant la Crèche du Secrétariat Général du Conseil (SGC) » (Dossier 2007-491)

**Évaluation du personnel — OEDT**

Avis du 11 janvier 2008 sur une notification en vue d'un contrôle préalable concernant « l'exercice d'évaluation du personnel » (Dossier 2007-334)

**Technologie des centres d'appels — OHMI**

Avis du 11 janvier 2008 sur une notification de contrôle préalable concernant la technologie des centres d'appel (Dossier 2007-583)

**Appel d'offres électronique — Conseil**

Avis du 10 janvier 2008 sur une notification concernant l'application d'appel d'offres électroniques dans le cadre des procédures de passation de marchés du Conseil (Dossier 2007-573)

**Base de données AGS-EDV au CCR ITU à Karlsruhe — Commission**

Avis du 10 janvier 2008 sur une notification de contrôle préalable à propos de la base de données AGS-EDV du Centre commun de recherche ITU, situé à Karlsruhe (Dossier 2007-378)

**Recrutements — Médiateur européen**

Avis du 9 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier « Recrutements des membres du personnel (fonctionnaires / temporaires / contractuels) » (Dossier 2007-405)

**Rapports de stage — Agence européenne pour la sécurité maritime**

Avis du 7 janvier 2008 sur la notification de contrôle préalable concernant les rapports de stage (Dossier 2007-569)

**Enregistrement des absences — Agence européenne des médicaments**

Avis du 7 janvier 2008 sur une notification de contrôle préalable concernant l'enregistrement des absences des agents temporaires, auxiliaires et contractuels, des experts nationaux et des stagiaires (Dossier 2007-420)

**Promotion — Comité des régions**

Avis du 7 janvier 2008 sur la notification d'un contrôle préalable à propos du dossier « Procédure de promotion des fonctionnaires » (Dossier 2007-354)

**Recrutement — Agence européenne pour la sécurité maritime**

Avis du 7 janvier 2008 sur la notification d'un contrôle préalable concernant le « recrutement d'agents permanents, temporaires et contractuels » (Dossier 2007-566)

## Annexe G

## Liste des avis sur des propositions législatives

**Stratégie européenne en matière de justice en ligne**

Avis du 19 décembre 2008 sur la communication de la Commission intitulée « Vers une stratégie européenne en matière d'e-Justice »

**Soins de santé transfrontaliers**

Avis du 2 décembre 2008 concernant la proposition de directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers

**Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations**

Avis du 11 novembre 2008 concernant le rapport final du Groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel

**Transparence du patrimoine des débiteurs**

Avis du 22 septembre 2008 sur le Livre vert de la Commission intitulé « Exécution effective des décisions judiciaires dans l'Union européenne : la transparence du patrimoine des débiteurs » – COM(2008) 128 final

**ECRIS**

Avis du 16 septembre 2008 sur la proposition de décision du Conseil relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2008/XX/JAI

**Accès du public aux documents**

Avis du 30 juin 2008 sur la proposition de règlement relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO C 2 du 7.1.2009, p. 7).

**Protection des enfants utilisant l'Internet**

Avis du 23 juin 2008 sur la proposition de décision instituant un programme communautaire pluriannuel visant à protéger les enfants lors de l'utilisation de l'Internet et d'autres technologies de communication (JO C 2 du 7.1.2009, p. 2)

**Statistiques européennes**

Avis du 20 mai 2008 sur la proposition de règlement relatif aux statistiques européennes (COM(2007) 625 final) (JO C 308 du 3.12.2008, p. 1)

**Sécurité routière**

Avis du 8 mai 2008 sur la proposition de directive du Parlement européen et du Conseil facilitant l'application transfrontière de la législation dans le domaine de la sécurité routière (JO C 310 du 5.12.2008, p. 9)

**Eurojust**

Avis du 25 avril 2008 sur l'initiative en vue de l'adoption d'une décision du Conseil sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI (JO C 310 du 5.12.2008, p. 1).

#### **Systèmes informatisés de réservation**

Avis du 11 avril 2008 sur la proposition de règlement instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation (JO C 233 du 11.9.2008, p. 1).

#### **Vie privée et communications électroniques**

Avis du 10 avril 2008 sur la proposition de directive modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») (JO C 181 du 18.7.2008, p. 1)

#### **Éléments de sécurité et éléments biométriques intégrés dans les passeports**

Avis du 26 mars 2008 concernant la proposition de règlement modifiant le règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres (JO C 200 du 6.8.2008, p. 1)

#### **Système d'information du marché intérieur (IMI)**

Avis du 22 février 2008 concernant la décision de la Commission du 12 décembre 2007 relative à la protection des données à caractère personnel dans le cadre de la mise en œuvre du Système d'information du marché intérieur (IMI) (2008/49/CE) (JO C 270 du 25.10.2008, p. 1)

## Annexe H

## Composition du secrétariat du CEPD

**Domaines placés sous la responsabilité directe du CEPD et du Contrôleur adjoint :**• **Supervision**

Sophie LOUVEAUX <i>Administrateur / Conseiller juridique</i> <i>Coordinatrice pour les relations avec les DPD et les contrôles préalables</i>	Delphine HAROU (*) <i>Assistante Supervision</i>
Rosa BARCELÓ <i>Administrateur / Conseiller juridique</i>	Xanthi KAPSOSIDERI <i>Assistante Supervision</i>
Zsuzsanna BELENYESSY <i>Administrateur / Conseiller juridique</i>	Sylvie LONGRÉE <i>Assistante Supervision</i>
Eva DIMOVNÉ KERESZTES <i>Administrateur / Conseiller juridique</i> <i>Coordinatrice pour les contrôles</i>	Kim Thien LÊ <i>Assistante Secrétariat</i>
Maria Veronica PEREZ ASINARI <i>Administrateur / Conseiller juridique</i> <i>Coordinatrice pour les mesures administratives</i>	Thomas GREMEL <i>Assistant Supervision</i>
Jaroslav LOTARSKI <i>Administrateur / Conseiller juridique</i> <i>Coordinateur pour les réclamations</i>	György HALMOS (*) <i>Expert national / Conseiller juridique</i> <i>(jusqu'en septembre 2008)</i>
Tereza STRUNCOVA <i>Administrateur / Conseiller juridique</i>	Athena BOURKA <i>Expert national / Conseiller Technologies</i> <i>(depuis septembre 2008)</i>
Isabelle CHATELIER <i>Administrateur / Conseiller juridique</i>	Manuel GARCIA SANCHEZ <i>Expert national / Conseiller Technologies</i> <i>(depuis septembre 2008)</i>

• **Politique et information**

Hielke HIJMANS <i>Administrateur / Conseiller juridique</i> <i>Coordinateur Consultation et procédures devant la Cour</i>	Nathalie VANDELLE (*) <i>Administrateur / Attachée de presse</i> <i>Coordinatrice équipe Information</i>
Laurent BESLAY <i>Administrateur / Conseiller Technologies</i> <i>Coordinateur Sécurité et technologies</i>	Martine BLONDEAU (*) <i>Assistante Documentation</i>
Bénédicte HAVELANGE <i>Administrateur / Conseiller juridique</i> <i>Coordinatrice Grands systèmes TI et politique des frontières</i>	Andrea BEACH <i>Assistante Secrétariat</i>
Alfonso SCIROCCO <i>Administrateur / Conseiller juridique</i>	Francisco Javier MOLEÓN GARCIA <i>Assistant Documentation</i>
Michaël VANFLETEREN <i>Administrateur / Conseiller juridique</i>	Gerard VAN BALLEGOIJ <i>Stagiaire (octobre 2008 à février 2009)</i>
Anne-Christine LACOSTE <i>Administrateur / Conseiller juridique</i> <i>Coordinatrice Groupe article 29</i>	Athina FRAGKOULI <i>Stagiaire (octobre 2008 à février 2009)</i>
Herke KRANENBORG <i>Administrateur / Conseiller juridique</i>	Sarah THOME <i>Stagiaire (octobre 2008 à février 2009)</i>
Katarzyna CUADRAT-GRZYBOWSKA <i>Administrateur / Conseiller juridique</i>	

(\*) Equipe Information



Le Contrôleur européen de la protection des données, le Contrôleur adjoint et leur personnel.

### **Unité Personnel / Budget / Administration**

Monique LEENS-FERRANDO

*Chef d'unité*

- **Ressources humaines**

Giuseppina LAURITANO  
*Administrateur / Conseillère Questions statutaires  
et Audits / Déléguée à la protection des données*

Anne LEVÉCQUE  
*Assistante Ressources humaines*

Vittorio MASTROJENI  
*Assistant Ressources humaines*

- **Budget et finances**

Tonny MATHIEU  
*Administrateur financier*

Maria SANCHEZ LOPEZ  
*Assistante Questions financières et Comptabilité*

Raja ROY  
*Assistante Questions financières et Comptabilité*

- **Administration**

Anne-Françoise REYNDERS  
*Activités sociales, Infrastructures, Assistante administrative*

## 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 (24.6.2004). Prorogation de cet accord signée le 11 décembre 2006.

### Liste des accords de niveau de service signés par le CEPD avec d'autres institutions :

- Accord de niveau de service 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 de niveau de service avec le Conseil ;
- Accord de niveau de service 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 24.6.2004, 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 l'évaluation 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 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 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 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 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

Règles du 16 juin 2008 relatives au remboursement des frais exposés par les personnes extérieures aux services du CEPD invitées à participer à des réunions en qualité d'expert

Décision du 8 août 2008 de l'ordonnateur délégué relative à l'archivage des documents financiers et des pièces justificatives

Décision du 2 octobre 2008 du contrôleur concernant les modalités d'application générale de l'article 45 bis du Statut (certification)

Décision du 16 décembre 2008 du contrôleur portant adoption de mesures de sécurité au sein du CEPD

Décision du 19 décembre 2008 du contrôleur portant nomination d'un responsable local de la sécurité au sein du CEPD

European Data Protection Supervisor

**Annual Report 2008**

Luxembourg: Office for Official Publications of the European Communities

2008 — 130 pp. — 21 × 29.7 cm

ISBN 978-92-79-11147-1



### **Comment vous procurer les publications de l'Union européenne ?**

#### **Publications payantes :**

- sur le site de l'EU Bookshop: <http://bookshop.europa.eu>;
- chez votre libraire, en lui donnant le titre, le nom de l'éditeur et/ou le numéro ISBN;
- en contactant directement un de nos agents de vente.

Vous obtiendrez leurs coordonnées en consultant

le site: HYPERLINK "http://bookshop.europa.eu" <http://bookshop.europa.eu>

ou par télécopie au numéro suivant: +352 2929-42758.

#### **Publications gratuites:**

- sur le site de l'EU Bookshop: <http://bookshop.europa.eu>;
- auprès des représentations ou délégations de la Commission européenne.

Vous obtiendrez leurs coordonnées en consultant le site: <http://ec.europa.eu>

ou par télécopie au numéro suivant: +352 2929-42758.



CONTRÔLEUR EUROPÉEN  
DE LA PROTECTION DES DONNÉES

*Le gardien européen  
de la protection des données personnelles*

**[www.edps.europa.eu](http://www.edps.europa.eu)**



Office des publications



9 789295 073036

ISBN 978-92-95073-03-6