ISSN 1830-5482

Rapport annuel 2009

Contrôleur européen de la protection des données

Rapport annuel

2009

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

Un numéro unique gratuit (*):

00 800 6 7 8 9 10 11

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

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

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

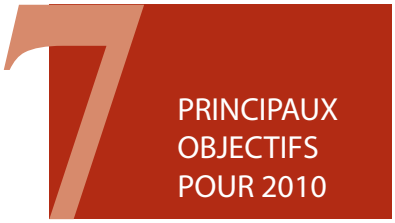
Luxembourg: Office des publications de l'Union européenne, 2011

ISBN 978-92-95073-04-3
doi:10.2804/12053

Printed in Luxembourg

IMPRIME SUR PAPIER BLANCHI SANS CHLORE ELEMENTAIRE (ECF)

Sommaire



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), et M. Giovanni Buttarelli, contrôleur adjoint, précédé de l'énoncé de leur mission.

Le chapitre 1 — **«Faits marquants de 2009»,** présente les grands axes des activités du CEPD en 2009 et les résultats obtenus dans les différents champs d'activité.

Le chapitre 2 — **«Contrôle»,** décrit les travaux menés pour vérifier que les institutions et organes de l'Union européenne (UE) s'acquittent de leurs obligations en matière de protection des données. Ce chapitre présente une analyse des principales problématiques dans le domaine des contrôles préalables, de la suite donnée aux réclamations et du contrôle du respect des règles et des avis sur les mesures administratives traitées en 2009. Il présente également les lignes directrices thématiques adoptées par le CEPD dans le domaine du recrutement, des données sur la santé et de la vidéosurveillance, ainsi qu'une mise à jour 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 leur incidence 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 forums importants, par exemple le groupe de l'article 29 (groupe sur la protection des données), les autorités de contrôle communes relevant du troisième pilier, ainsi que la Conférence européenne et 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 les activités de communication extérieure avec les médias et l'information du public.

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 chapitre 7 — **«Principaux objectifs pour 2010»** fournit un aperçu des priorités principales pour 2010.

Le rapport est complété par des annexes, dans lesquelles figurent un aperçu du cadre juridique pertinent, les dispositions du règlement (CE) n° 45/2001, la liste des délégués à la protection des données, la liste des avis et avis consultatifs relatifs aux contrôles préalables, les discours prononcés par le contrôleur et son adjoint et la composition du secrétariat du CEPD.

Le présent rapport existe également sous la forme d'une synthèse qui propose une version concise des principaux faits intervenus en 2009 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), où vous pourrez vous inscrire pour recevoir notre newsletter.

Il est possible de commander auprès de l'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 a pour mission de veiller à ce que les institutions et organes de l'Union respectent les droits et libertés fondamentaux des personnes lorsqu'ils traitent des données à caractère personnel.

Le CEPD est chargé de:

- superviser et d'assurer le respect des dispositions du règlement (CE) n° 45/2001 ([1]) et des autres actes communautaires relatifs à la protection des droits fondamentaux et des libertés lorsque les institutions et organes de l'UE 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 des 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 de l'ancien 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 de l'Union, et de contribuer ainsi à améliorer la bonne gouvernance;

- d'intégrer, selon les nécessités, le respect des principes de protection des données dans la législation et la politique de l'Union;

- d'améliorer la qualité des politiques de l'UE, chaque fois que la protection effective des données personnelles est une condition essentielle du succès de ces politiques.

([1]) 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).

Peter Hustinx, Contrôleur européen de la protection des données et Giovanni Buttarelli, Contrôleur adjoint.

AVANT-PROPOS

Nous avons l'honneur de présenter au Parlement européen, au Conseil et à la Commission le rapport annuel sur les activités du Contrôleur européen de la protection des données, conformément au règlement (CE) n° 45/2001 du Parlement européen et du Conseil, et en application de l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), qui a remplacé l'article 286 du traité instituant la Communauté européenne (CE).

Le présent rapport couvre l'année 2009, cinquième 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 de l'Union. Ce rapport couvre également la première année de notre mandat commun de cinq ans, en tant que membres actuels de cette autorité.

Cette année a revêtu une importance cruciale pour le droit fondamental à la protection des données en raison de quelques évolutions majeures: l'entrée en vigueur du traité de Lisbonne, garantissant une base juridique solide pour une protection globale des données dans tous les domaines de la politique de l'UE; le lancement d'une consultation publique sur l'avenir du cadre juridique de protection des données de l'UE, et l'adoption d'un nouveau programme politique de cinq ans dans le domaine de la liberté, de la sécurité et de la justice («programme de Stockholm») mettant un accent considérable sur la protection des données en tant qu'élément essentiel assurant la légitimité et l'efficacité dans ce domaine.

Le CEPD est fortement engagé dans ces domaines et est déterminé à poursuivre dans cette voie à l'avenir. En même temps, nous avons fait en sorte que la fonction d'autorité de contrôle indépendante soit exercée dans tous les domaines d'activité habituels. Cela a débouché sur des progrès importants, à la fois en ce qui concerne le contrôle des institutions et organes de l'UE lorsqu'ils traitent des données personnelles, la consultation sur les nouvelles politiques et mesures législatives et la collaboration étroite avec d'autres autorités de contrôle, afin de garantir une plus grande cohérence en matière de protection des données.

Nous souhaitons donc profiter de l'occasion qui nous est donnée 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 des divers organes qui sont responsables de la manière dont la protection des données est mise en pratique. Nous encourageons également tous ceux qui sont chargés de relever les défis de demain.

Enfin, nous souhaitons tout particulièrement remercier les membres de notre personnel. Par leurs qualités exceptionnelles, ces derniers contribuent largement à l'efficacité de notre action.

Peter Hustinx
Contrôleur européen de la protection des données

Giovanni Buttarelli
Contrôleur adjoint

1

FAITS MARQUANTS DE 2009

1.1. Éléments clés

Certains développements de 2009 ont conduit à renforcer l'attention portée au droit fondamental à la protection des données à caractère personnel et à développer des moyens modernes permettant de garantir, en pratique, une protection des données à caractère personnel plus efficace. Cette attention accrue est la bienvenue dans la perspective des défis constitués par les nouvelles technologies, la mondialisation et les intérêts publics contradictoires.

L'entrée en vigueur du traité de Lisbonne en décembre 2009 a donné une base juridique solide à la protection globale des données dans tous les domaines de la politique de l'UE. La charte des droits fondamentaux a acquis la même valeur juridique que les traités. Cela vaut également pour son article 8 relatif à la protection des données à caractère personnel. L'article 16 du traité sur le fonctionnement de l'Union européenne prévoit désormais — entre autres dispositions générales du traité — un droit directement exécutoire à la protection des données à caractère personnel.

L'article 16 TFUE fournit également une base juridique générale pour les règles relatives à la protection des individus à l'égard du traitement des données à caractère personnel par les institutions et organes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. Le respect de ces règles est soumis au contrôle d'autorités indépendantes, comme le prévoit également l'article 8 de la charte. Cela permettra — et nécessitera — une révision complète du cadre juridique en vigueur en matière de protection des données, afin de garantir que toute personne couverte par la juridiction de l'UE bénéficie pleinement du droit fondamental à la protection des données.

Le deuxième développement clé a été la décision de la Commission européenne de mettre en œuvre une consultation publique sur l'avenir du cadre juridique européen en vigueur en matière de protection des données, avant même que l'entrée en vigueur du traité de Lisbonne ne devienne une réalité juridique et politique.

Cela s'est manifesté par une conférence publique en mai 2009 et une consultation publique de juillet à décembre 2009. Le contrôleur et le contrôleur adjoint ont tous deux contribué personnellement à la conférence. Ils se sont également montrés très actifs, avec leurs collègues du groupe de travail de l'article 29 et du groupe de travail sur la police et la justice pour apporter une contribution conjointe à la consultation publique, permettant à la Commission d'élaborer un cadre juridique global pour tous les domaines de la politique de l'UE et pour garantir son efficacité pratique, en dépit de tous les défis à relever.

La contribution conjointe des deux groupes de travail, adoptée avec le soutien entier et actif du contrôleur européen de la protection des données en décembre 2009, a été l'une des plus importantes soumises à la consultation publique. Le CEPD continuera de suivre cette question de très près

à l'avenir et sera disponible pour fournir d'autres avis si nécessaire.

Le troisième développement majeur a été l'adoption d'un nouveau programme d'action de cinq ans relatif à l'espace de liberté, de sécurité et de justice («programme de Stockholm»), mettant l'accent sur la protection des données en tant qu'élément essentiel pour arriver à une certaine légitimité et à une efficacité dans ce domaine peu après l'entrée en vigueur du traité de Lisbonne, également en décembre 2009. Ce programme examine l'incidence du traité de Lisbonne dans ce domaine et établit les lignes d'action principales de la politique de l'UE pour les cinq prochaines années. Sa mise en œuvre bénéficiera également des changements institutionnels prévus par le traité de Lisbonne.

L'échange de données à caractère personnel entre les autorités chargées de la migration, de la répression et de la sécurité publique dans les différents États membres fait partie intégrante de cette politique. L'assurance que cette protection des données sera «intégrée» à ces politiques et à ces systèmes dès le départ est un engagement important, soutenu et encouragé activement par le CEPD, qui continuera de contrôler à quel moment et à quel endroit cela sera appliqué pratiquement.

Ces différents développements ont encore plus de poids lorsqu'ils coïncident avec le début d'une nouvelle Commission en février 2010, ce qui met également un accent considérable sur la protection des droits fondamentaux en général, et en particulier sur la protection des données à caractère personnel, qui se voit accorder une priorité élevée. En ce qui concerne les défis mentionnés plus haut, il convient de dire qu'ils découlent en grande partie de la dépendance sans cesse croissante de la société envers l'utilisation répandue des technologies de l'information (TI) dans de nombreux domaines de l'existence.

Comme cette tendance se poursuivra probablement et deviendra même encore plus pertinente dans le contexte de l'agenda numérique de la Commission, il convient de souligner la nécessité de parvenir prochainement à une protection plus efficace et plus globale des données à caractère personnel. Le CEPD se réjouit des propositions de la Commission dans tous les domaines concernés et les évaluera très attentivement en temps opportun.

1.2. Aperçu général de 2009

Les principales activités du CEPD en 2009 ont été fondées sur la même stratégie globale que précédemment, mais leur importance et les domaines couverts ont continué de se développer. L'aptitude du CEPD à agir efficacement s'est également améliorée.

Le cadre juridique ([2]) dans lequel le CEPD opère définit un certain nombre de tâches et de compétences qui dessinent les contours de 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 contrôler et assurer le respect des garanties juridiques existantes par les institutions et organes de l'UE ([3]) chaque fois qu'ils traitent des données à caractère personnel;

- une fonction de consultation, qui consiste à conseiller les institutions et organes de l'UE 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 de l'ancien troisième pilier de l'UE chargés de la coopération policière et judiciaire en matière pénale, en vue d'améliorer la cohérence en ce qui concerne la protection des données à caractère personnel.

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 2009. Certains éléments clés seront résumés dans ce chapitre.

L'importance de l'information et de la communication pour ces activités nous a amenés à consacrer un chapitre à cet aspect de la question (voir le

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

([3]) 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 de l'UE. Pour obtenir une liste complète de celles-ci, utilisez le lien: http://europa.eu/agencies/community_agencies/index_fr.htm.

chapitre 5). Toutes ces activités reposent sur une gestion efficace des ressources financières, humaines et autres, qui font l'objet du chapitre 6.

Supervision

Les tâches de supervision vont du conseil et de l'aide aux délégués à la protection des données, à la conduite d'enquêtes, notamment des enquêtes sur le terrain et le traitement des réclamations, en passant par le contrôle préalable des opérations de traitement des données à risque. Les avis complémentaires à l'administration de l'UE peuvent également prendre la forme de consultations sur les mesures administratives ou de publication de lignes directrices thématiques.

Toutes les institutions et tous les organes de l'UE doivent posséder au moins un délégué à la protection des données. En 2009, le nombre total de délégués à la protection des données est passé à 45. Il est important, pour une supervision efficace, d'interagir régulièrement avec ces délégués et leurs réseaux.

En 2009, le contrôle préalable des opérations de traitement à risques a encore constitué l'essentiel des activités de supervision. Le CEPD a adopté 110 avis de contrôle préalable sur les données de santé, l'évaluation du personnel, le recrutement, la gestion du temps, l'enregistrement téléphonique, les outils de performance et les enquêtes de sécurité. Ces avis sont publiés sur le site du CEPD et leur mise en œuvre fait l'objet d'un suivi systématique.

La mise en œuvre du règlement par les institutions et organes fait également l'objet d'un suivi systématique par le biais d'un bilan régulier des indicateurs de performance associant toutes les institutions et tous les organes de l'UE. À la suite de l'exercice «printemps 2009», le CEPD a publié un rapport indiquant que les institutions de l'UE avaient accompli des progrès considérables en matière de réponse aux exigences de protection des données. Toutefois, le niveau de conformité est plus faible dans la plupart des agences.

Le CEPD a également effectué quatre enquêtes sur place dans différents organes et institutions. Ces enquêtes font systématiquement l'objet d'un suivi et seront de plus en plus fréquentes à l'avenir. En juillet 2009, le CEPD a adopté un manuel de procédure d'enquêtes et publié les éléments essentiels de cette procédure sur son site internet.

En 2009, le nombre total des réclamations reçues s'élevait à 111, dont 42 seulement ont été jugées recevables. De nombreuses réclamations irrecevables concernaient des problématiques nationales, pour lesquelles le CEPD n'est pas compétent. La plupart des questions couvertes par les réclamations recevables avaient trait à des violations présumées de la confidentialité, à une collecte excessive de données ou à l'utilisation illégale de données par le contrôleur. Dans 8 cas, le CEPD a conclu à une violation des règles de protection des données.

Des travaux ont également été effectués sous la forme d'une consultation sur les mesures administratives envisagées par les institutions et organes de l'UE concernant le traitement des données à caractère personnel. Diverses questions ont été évoquées, notamment sur les transferts de données vers des pays tiers ou des organisations internationales, le traitement des données en cas de pandémie, la protection des données au sein du service d'audit interne (SAI) et les modalités d'application du règlement (CE) n° 45/2001.

Le CEPD a adopté des lignes directrices sur le traitement des données à caractère personnel pour le recrutement et sur les données relatives à la santé sur le lieu de travail. En 2009, le CEPD a également organisé une consultation publique sur les lignes directrices relatives à la vidéosurveillance, insistant entre autres sur la «prise en considération du respect de la vie privée dès la conception» (*Privacy by Design*) et la responsabilité, qui font figure de principes essentiels dans ce contexte.

Chiffres clés du CEPD en 2009

➔ **110 avis de contrôle préalable adoptés** concernant des données de santé, l'évaluation du personnel, le recrutement, la gestion du temps, les enquêtes de sécurité, les enregistrements téléphoniques et les outils de performances.

➔ **111 réclamations reçues, dont 42 recevables.** Principaux types de violations présumées: violation de la confidentialité des données, collecte excessive de données ou utilisation illégale des données par le contrôleur.

- **12 affaires résolues** dans lesquelles le CEPD n'a constaté aucune violation des règles de protection des données.
- **8 violations déclarées** des règles de protection des données.

➔ **32 consultations sur les mesures administratives.** Des conseils ont été donnés sur toute une série d'aspects juridiques liés au traitement des données personnelles par les institutions et organes de l'UE.

➔ **4 enquêtes sur place effectuées** dans divers organes et institutions de l'UE.

➔ **3 lignes directrices publiées** sur le recrutement, les données de santé et la vidéosurveillance.

➔ **16 avis législatifs publiés** sur les systèmes d'information à grande échelle, les listes terroristes, le futur cadre de protection des données, la santé publique, la fiscalité et les transports.

➔ **4 ensembles de commentaires formels** sur l'accès du public aux documents, le service universel et la vie privée dans les communications électroniques, ainsi que sur les négociations entre l'Union et les États-Unis concernant le nouvel accord SWIFT.

➔ **3 réunions du groupe de supervision et de coordination Eurodac,** qui ont eu pour résultat un deuxième rapport d'inspection coordonné sur les informations des personnes concernées et l'évaluation de l'âge des jeunes demandeurs d'asile.

Consultation

Plusieurs événements importants ont contribué à nous rapprocher d'un nouveau cadre juridique de protection des données. Y parvenir sera l'un des thèmes dominants de l'agenda du CEPD pour les années à venir.

À la fin de 2008, un cadre juridique général de protection des données dans le domaine de la coopération policière et judiciaire a été adopté au niveau de l'UE. Même s'il n'est pas parfait, il constituait un pas important dans la bonne direction.

En 2009, un deuxième développement majeur a été l'adoption de la directive «Vie privée et communications électroniques» révisée dans le cadre d'un paquet plus large. Cela a également été un premier pas vers la modernisation du cadre juridique de protection des données.

L'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, a non seulement conféré un caractère contraignant à la charte des droits fondamentaux pour les institutions et les organes, ainsi que pour les États membres agissant dans le cadre du droit de l'UE, mais a également permis l'introduction d'une base générale de cadre juridique global au titre de l'article 16 TFUE.

En 2009, la Commission a également lancé une consultation publique sur l'avenir du cadre juridique de la protection des données. Le CEPD a travaillé étroitement avec ses collègues pour garantir un apport conjoint adéquat à la consultation et a souligné à plusieurs reprises la nécessité d'une protection des données plus vaste et plus efficace dans l'Union européenne.

Le CEPD a continué à mettre en œuvre sa politique de consultation générale et a publié un nombre record d'avis législatifs sur différents sujets. Cette politique garantit également une approche proactive, incluant un inventaire régulier des propositions législatives à soumettre à la consultation, ainsi que la disponibilité de commentaires informels lors des étapes préparatoires des propositions législatives. La plupart des avis du CEPD ont été suivis par des discussions au Parlement et au Conseil.

En 2009, le CEPD a suivi avec un intérêt particulier les développements concernant le programme de Stockholm et ses perspectives pour les cinq prochaines années dans le domaine de la justice et des affaires intérieures. Le CEPD a émis un avis sur le développement du programme et a participé aux travaux préparatoires pour le modèle européen d'information.

D'autres travaux dans ce domaine ont porté sur la révision des règlements Eurodac et Dublin, la création d'une agence pour la gestion opérationnelle de systèmes d'information à grande échelle et une

approche cohérente de la supervision dans ce domaine.

Dans le contexte de la directive «Vie privée et communications électroniques», hormis la révision générale mentionnée plus haut, le CEPD s'est penché sur des questions concernant la directive relative à la conservation des données, sur l'utilisation des étiquettes RFID (identification par radiofréquence) ou des systèmes de transport intelligents et sur le rapport de l'organe consultatif Riseptis intitulé *«Trust in the Information Society»* (la confiance dans la société de l'information).

Dans le contexte de la mondialisation, le CEPD a participé au développement de normes mondiales, au dialogue transatlantique sur la protection des données et les données détenues par les services répressifs, ainsi que sur des questions liées aux mesures restrictives à l'égard des terroristes présumés et de certains pays tiers.

Les autres domaines présentant un intérêt pour le CEPD sont la santé publique — notamment les soins de santé transfrontaliers, l'e-santé et la pharmacovigilance — ainsi que l'accès du public aux documents —, notamment la révision du règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents, et différentes affaires judiciaires concernant la relation entre l'accès du public et la protection des données.

Coopération

La principale plate-forme de coopération entre les autorités de protection des données (APD) en Europe est le groupe de l'article 29. Le CEPD participe à ses activités et joue ainsi un rôle important dans l'application uniforme de la directive relative à la protection des données.

Le CEPD et le groupe de l'article 29 coopèrent en parfaite synergie sur toute une série de sujets, en particulier en ce qui concerne la mise en œuvre de la directive relative à la protection des données et les défis posés par les nouvelles technologies. Le CEPD a également fortement soutenu les initiatives visant à faciliter les flux de données transfrontaliers.

Il convient de mentionner tout particulièrement la contribution conjointe sur l'avenir de la protection de la vie privée, en réponse à la consultation de la Commission européenne sur le cadre juridique de protection des données de l'UE, et à la consultation de la Commission sur l'impact des scanners corporels dans le domaine de la sécurité de l'aviation.

L'une des tâches de coopération les plus importantes du CEPD concerne Eurodac. La responsabilité de la supervision est ici partagée avec les autorités nationales de protection des données. Le groupe de coordination du contrôle d'Eurodac — composé de représentants des autorités nationales chargées de la protection des données et du CEPD — s'est réuni trois fois et s'est concentré sur la mise en œuvre du programme de travail adopté en décembre 2007.

L'un des principaux résultats a été l'adoption, en juin 2009, d'un deuxième rapport d'inspection consacré à deux questions: le droit à l'information pour les demandeurs d'asile et les méthodes d'évaluation de l'âge des jeunes demandeurs d'asile.

Le CEPD a poursuivi une étroite coopération avec les autorités de protection des données de l'ancien «troisième pilier» — espace de coopération policière et judiciaire — et avec le groupe de travail sur la police et la justice. En 2009, cela s'est notamment concrétisé par des contributions au débat sur le programme de Stockholm et l'évaluation de l'impact de la décision-cadre du Conseil sur la protection des données.

La coopération dans les autres forums internationaux a continué d'attirer l'attention, surtout la 31e conférence internationale des commissaires à la protection des données et de la vie privée, qui a conduit à l'adoption d'un ensemble de normes mondiales en matière de protection des données.

Le CEPD a également organisé un atelier intitulé «Faire face aux failles de sécurité» dans le cadre de l'«initiative de Londres» portée sur les fonts baptismaux lors de la 28e conférence internationale de novembre 2006 en vue de sensibiliser à la protection des données et à rendre celle-ci plus efficace.

1.3. Résultats obtenus en 2009

Le rapport annuel 2008 exposait les principaux objectifs ci-après, qui avaient été retenus pour l'année 2009. 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 de soutenir pleinement les délégués à la protection des données, en particulier dans les agences créées récemment, et les a encouragés

à poursuivre les échanges de compétences et de bonnes pratiques afin de renforcer leur efficacité.

- Rôle du contrôle préalable

Le CEPD a pratiquement achevé le contrôle préalable des opérations de traitement en cours pour la plupart des institutions et organes existant de longue date et a placé un accent accru sur le suivi des recommandations. Le contrôle préalable des opérations de traitement communes dans les agences a fait l'objet d'une attention particulière.

- Lignes directrices horizontales

Le CEPD a publié des lignes directrices sur le recrutement du personnel et les données relatives à la santé au travail, ainsi que des projets de lignes directrices sur la vidéosurveillance, qui ont fait l'objet d'une consultation. Ces lignes directrices visent à assurer le respect des règles dans les institutions et les organes et à rationaliser les procédures de contrôle préalable.

- Traitement des réclamations

Le CEPD a adopté un manuel de traitement des réclamations à l'intention de son personnel et en a publié les grandes lignes sur son site internet 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. Un formulaire de réclamation est désormais disponible sur le site internet.

- Politique d'enquêtes

Le CEPD a continué de vérifier le respect du règlement (CE) n° 45/2001 au moyen de différents types de contrôles concernant tous les organes et institutions et a effectué un certain nombre d'enquêtes sur le terrain. Une première série de procédures d'enquête a été publiée pour garantir un processus plus prévisible.

- Étendue des consultations

Le CEPD a rendu un nombre record de seize avis et formulé quatre ensembles d'observations formelles sur les propositions de nouvelles législations, sur la base d'un inventaire, établi de façon systématique, des priorités et sujets pertinents. Il en a également assuré un suivi approprié. Tous les avis et observations, ainsi que l'inventaire, sont disponibles sur son site internet.

- Programme de Stockholm

Le CEPD a accordé 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 adopté par le Conseil à la fin 2009. La nécessité d'une protection efficace des données a été reconnue en tant que condition essentielle.

- Activités d'information

Le CEPD a amélioré la qualité et l'efficacité des outils d'information en ligne (site internet et lettre d'information électronique) et a procédé, le cas échéant, à une actualisation de ses autres activités d'information (nouvelle brochure d'information et activités de sensibilisation).

- Règlement intérieur

Le règlement intérieur, qui définira les différentes activités du CEPD, sera adopté prochainement. Il confirmera ou clarifiera principalement les pratiques actuelles et sera disponible sur le site internet.

- Gestion des ressources

Le CEPD a consolidé et continué de développer ses activités liées aux ressources financières et humaines. Il a accordé une attention particulière au recrutement de personnel par le biais d'un concours de l'Office européen de sélection du personnel (EPSO) en matière de protection des données. Les premiers lauréats devraient être connus dans le courant de 2010.

2

SUPERVISION

2.1. Introduction

La mission du CEPD, en sa qualité de contrôleur indépendant, consiste à surveiller le traitement des données à caractère personnel effectué par les institutions et organes de l'UE, relevant en tout ou en partie du champ d'application de ce qu'on appelait le «droit communautaire» ([4]) (à l'exclusion de la Cour de justice dans l'exercice de ses fonctions juridictionnelles). Le règlement (CE) n° 45/2001 (ci-après «le règlement») définit et confère un certain nombre de fonctions et de compétences qui permettent au CEPD de s'acquitter de sa tâche.

Le traité de Lisbonne constitue un changement de cadre juridique pour la protection des données dans l'administration européenne avec l'introduction de l'article 16 TFUE, qui remplace l'article 286 du traité CE. Les implications précises de ce changement et de la suppression de la structure en piliers des activités de supervision du CEPD sont actuellement examinées et pourraient nécessiter des éclaircissements supplémentaires.

Le contrôle préalable des opérations de traitement a continué d'être un élément important de la supervision en 2009 (voir la section 2.3), mais le CEPD s'est également attelé à d'autres formes de supervision, telles que le traitement des réclamations, les enquêtes, les avis sur les mesures administratives et la rédaction de lignes directrices thématiques. La supervision d'Eurodac est une activité spécifique du CEPD.

En 2009, comme au cours des années précédentes, le CEPD n'a ordonné aucune mesure et n'a émis aucun avertissement ni interdiction, les responsables du traitement ayant mis en œuvre ses recommandations ou exprimé leur intention de le faire en prenant les mesures nécessaires à cette fin. Toutefois, la rapidité de réaction varie d'un cas à l'autre.

2.2. Délégués à la protection des données

Un élément intéressant du paysage de la protection des données dans les institutions de l'Union européenne est l'obligation de désigner un délégué à la protection des données (DPD) (article 24, paragraphe 1, du règlement). Certaines institutions ont associé à ce DPD 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). Plusieurs institutions ont également nommé des coordinateurs de la protection des données chargés de coordonner tous les aspects de la protection des données au sein d'une direction ou unité particulière.

En 2009, 7 nouveaux DPD ont été nommés dans des nouvelles agences ou des entités conjointes, ce qui porte leur nombre total à 45.

([4]) Article 3, paragraphe 2, du règlement (CE) n° 45/2001.

Depuis plusieurs années, les DPD se rencontrent régulièrement afin d'échanger leurs expériences et d'examiner des questions horizontales. Ce réseau informel a fait la preuve de son efficacité en termes de collaboration, ce qui a continué d'être le cas en 2009.

Un «quatuor de délégués à la protection des données», composé de quatre DPD [Conseil, Parlement européen, Commission européenne et Centre de traduction des organes de l'Union européenne (CdT)] a été désigné afin de coordonner le réseau des DPD. Le CEPD a étroitement collaboré avec ce quatuor.

Le CEPD a assisté aux réunions que les DPD ont tenues en mars 2009 à la Banque centrale européenne (BCE) et en octobre 2009 à la Commission européenne (coorganisées par l'OLAF) et en a profité pour informer les DPD sur ses activités, pour présenter un aperçu des derniers développements en matière de protection des données dans l'UE et pour discuter des questions d'intérêt commun.

En particulier, le CEPD a mis ce forum à profit pour expliquer et débattre de la procédure de contrôle préalable, pour rendre compte de l'évolution des notifications en vue d'un contrôle préalable, pour informer les DPD sur l'exercice «printemps 2009» et son suivi (voir la section 2.5), pour fournir des informations sur ses enquêtes et pour présenter sa politique et sa procédure d'enquête. Le CEPD a également profité de cette occasion pour relancer les travaux sur l'établissement de normes professionnelles pour les DPD et pour échanger des informations au sujet des initiatives prises au cours de la Journée européenne de la protection des données (28 janvier).

Les délégués à la protection des données lors de leur 26e réunion, à Bruxelles (octobre 2009).

2.3. Contrôles préalables

2.3.1. Base juridique

L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 prévoit 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 leur finalité» doivent être soumis au contrôle préalable du CEPD. Celui-ci estime, par exemple, que la présence de certaines données biométriques autres que de simples photos présente des risques spécifiques pour les droits et libertés des personnes concernées et justifie un contrôle des activités de traitement par le CEPD. Ces avis se basent principalement sur la nature sensible des données biométriques.

L'article 27, paragraphe 2, du règlement dresse une liste non exhaustive des opérations de traitement susceptibles de présenter des risques. Les critères élaborés au cours des années précédentes ([5]) ont continué d'être appliqués pour l'interprétation de cette disposition, tant pour décider qu'un cas notifié par un DPD ne devait pas faire l'objet d'un contrôle préalable que pour émettre un avis dans le cadre d'une consultation sur la nécessité de procéder à un tel contrôle (voir le point 2.3.4).

([5]) Voir le rapport annuel 2005, point 2.3.1.

2.3.2. Procédure

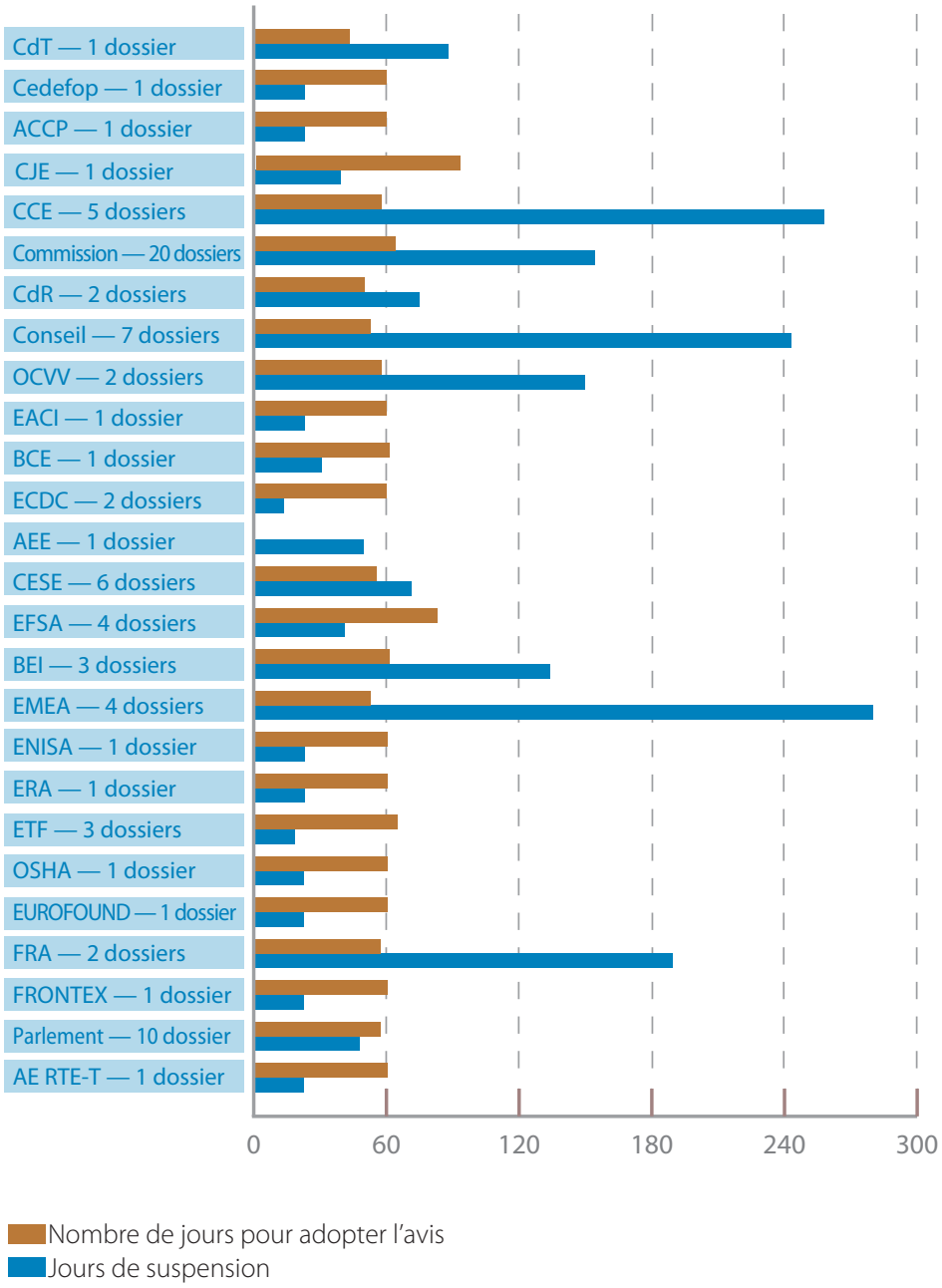
Notification

Les contrôles préalables doivent être effectués par le CEPD après réception de la notification du DPD. Si celui-ci s'interroge sur la nécessité de soumettre une opération de traitement à un contrôle préalable, il peut consulter le CEPD (voir le point 2.3.4).

Les contrôles préalables ne concernent pas uniquement les opérations qui ne sont pas encore en cours, mais aussi les traitements qui ont commencé avant le 17 janvier 2004 (date de nomination du CEPD et de son adjoint) ou avant l'entrée en vigueur du règlement (contrôles préalables a posteriori). Dans ces situations, un contrôle dans le cadre de l'article 27 ne peut être «préalable» au sens strict du terme, mais doit être traité a posteriori.

Délai, suspension et prolongation

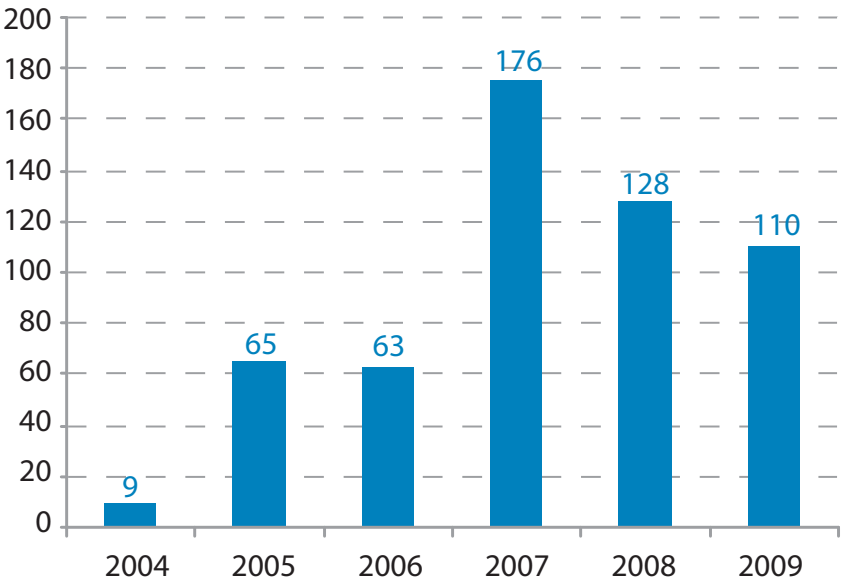
Délai moyen par institution/agence



Le CEPD doit rendre son avis dans les deux mois qui suivent la réception d'une notification ([6]). Lorsqu'il demande des informations complémentaires, le délai de deux mois est généralement suspendu jusqu'à ce que les informations en question lui aient été communiquées. Cette période de suspension comprend le délai accordé au DPD pour formuler ses observations et fournir, le cas échéant, des informations complémentaires sur le projet final. Lorsque la complexité du dossier l'exige, le CEPD peut également prolonger la période initiale de deux mois. Si, au terme de ce délai 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.

Registre

Notifications au CEPD



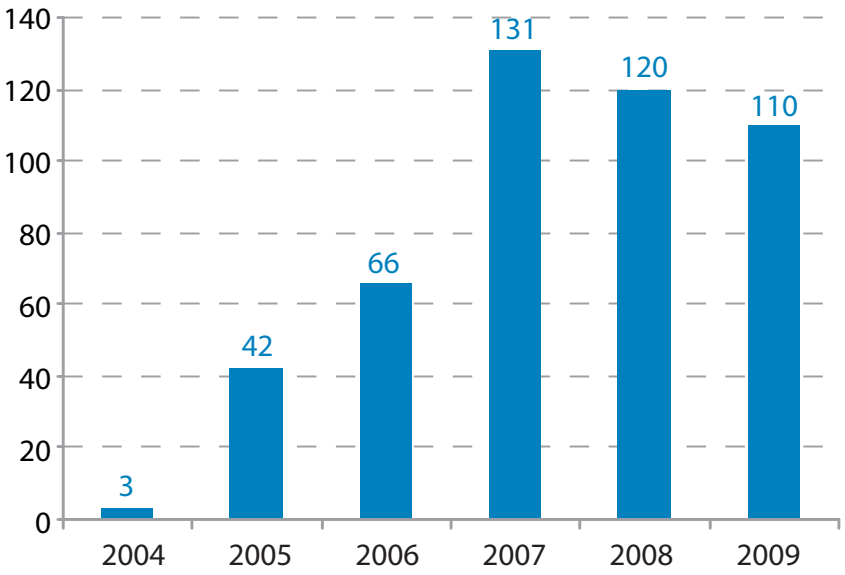
En 2009, le CEPD a reçu 110 notifications pour contrôle préalable, soit une légère baisse par rapport à 2008, étant donné que le CEPD arrive au bout de l'arriéré des dossiers de contrôle préalable a posteriori.

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. Par souci de transparence, toutes les informations sont consignées dans le registre disponible sur le site internet du CEPD (à l'exception des mesures de sûreté, qui ne sont pas mentionnées dans le registre).

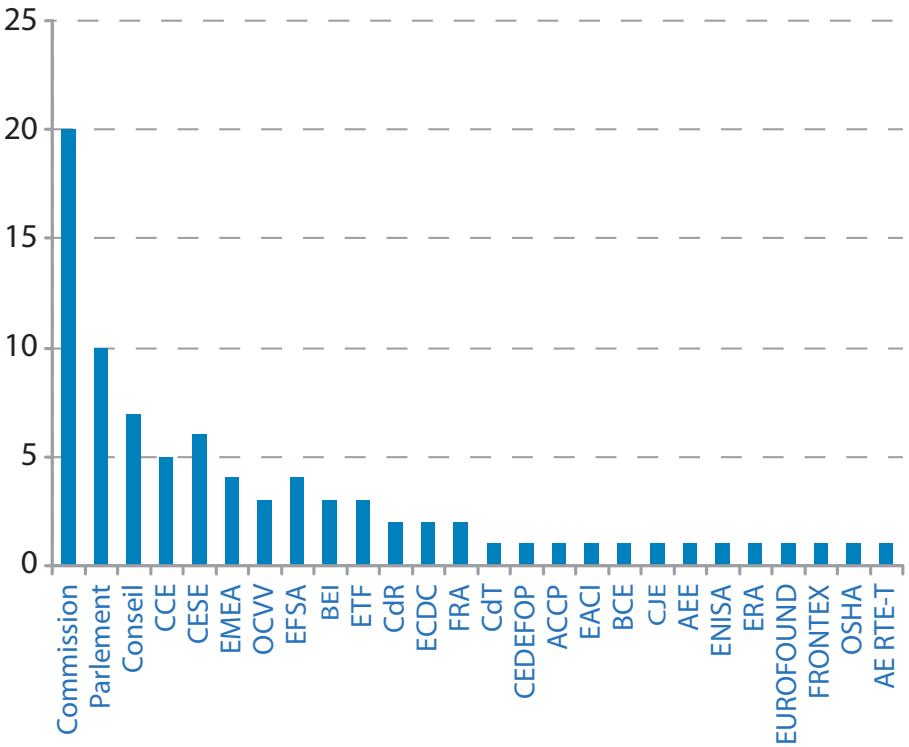
([6]) Pour les cas examinés a posteriori reçus avant le 1er septembre 2009, le mois d'août a été exclu des calculs, tant pour les institutions/organes que pour le CEPD.

Avis

Nombre d'avis du CEPD en vue d'un contrôle préalable par an



Nombre d'avis du CEPD en vue d'un contrôle préalable par institution en 2009



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. **En 2009, le CEPD a rendu 110 avis sur des notifications en vue d'un contrôle préalable** (voir ci-dessus, le graphique «Nombre d'avis du CEPD en vue d'un contrôle préalable par an»), ce qui représente une faible baisse par rapport aux deux années précédentes.

La **majorité de ces avis** concerne les **plus grandes institutions,** 20 concernant le traitement à la Commission européenne, 10 au Parlement européen et 7 au Conseil (voir ci-dessus, le graphique intitulé «Nombre d'avis du CEPD en vue d'un contrôle préalable par institution en 2009»). De nombreuses agences ont également commencé à notifier leurs activités principales et des procédures administratives standard conformément aux procédures établies par le CEPD (voir le point 2.3.2).

Les avis contiennent une description de la procédure, un résumé des faits et une analyse juridique visant à déterminer si le traitement respecte les dispositions applicables du règlement. Si nécessaire, des recommandations sont formulées à l'intention du responsable du traitement en vue de garantir le respect du règlement. Dans ses conclusions, le CEPD déclare généralement que le traitement ne paraît pas entraîner de violation d'une disposition quelconque du règlement, pour autant qu'il soit tenu compte des recommandations émises.

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.

Un manuel garantit que l'ensemble de l'équipe s'appuie sur des bases 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. 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 2.3.6).

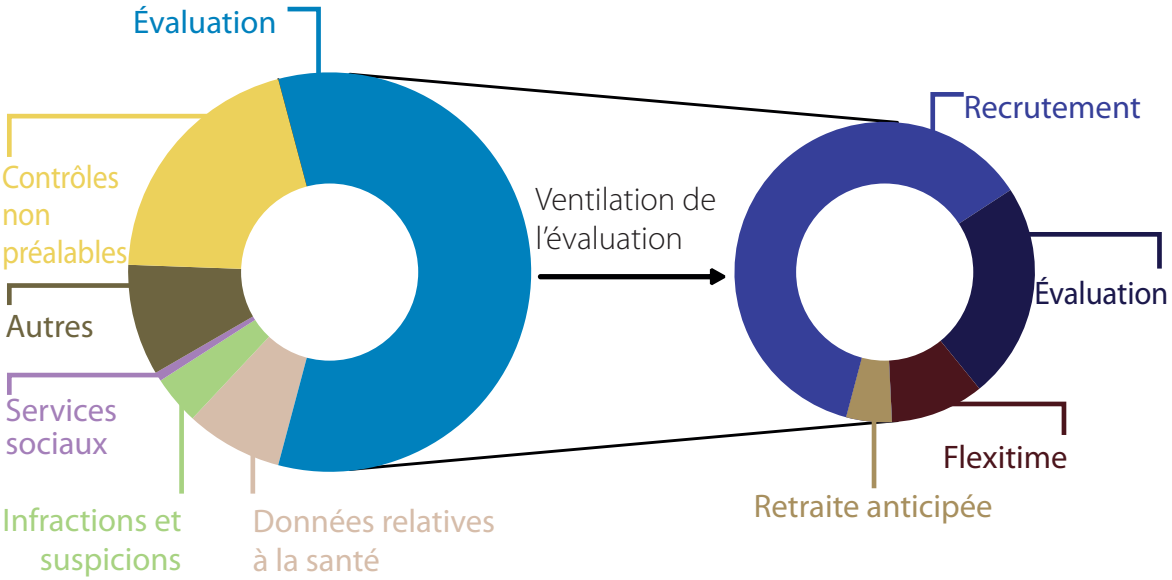
Procédure applicable aux contrôles préalables a posteriori dans les agences

En octobre 2008, le CEPD a lancé 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» axé uniquement sur les spécificités d'une agence. Pour aider les agences à établir 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 (voir ci-dessous, «2.7 Lignes directrices thématiques»). Le DPD soumettra ensuite une notification au sens de l'article 27, assortie d'une note soulignant les aspects particuliers au regard de la position du CEPD dans ce domaine (particularités du traitement au sein de l'agence, questions posant problème, etc.).

Le premier thème était le **recrutement,** qui a fait l'objet d'un avis horizontal du CEPD en mai 2009, couvrant les notifications de 12 agences. Un deuxième ensemble de lignes directrices a été envoyé aux agences à la fin de septembre 2009 concernant le traitement des données relatives à la santé. Le processus de réception des notifications par le CEPD était toujours en cours dans ce domaine avant l'adoption d'un avis horizontal au début de 2010.

2.3.3. Principales questions liées aux contrôles préalables

Avis rendus en 2009 par catégorie



Données médicales et autres données relatives à la santé

Les institutions et agences européennes traitent des données médicales et autres données relatives à la santé des individus dans plusieurs situations liées à l'application du statut des fonctionnaires (examen médical prérecrutement, examen médical annuel, remboursement des frais médicaux, certificats médicaux justifiant les congés de maladie, etc.). En raison de la nature particulièrement sensible des données relatives à la santé, les opérations de traitement de ces données sont soumises à un contrôle préalable du CEPD.

En 2009, le CEPD a continué à adopter plusieurs avis dans le domaine des données relatives à la santé (voir le graphique ci-dessus).

En septembre 2009, le CEPD a publié des lignes directrices sur le traitement de ces données en vue de l'analyse des notifications des opérations de traitement des données relatives à la santé par les agences de l'UE (voir ci-dessous, «2.7 Lignes directrices thématiques»). Ces lignes directrices constituent également un ensemble de normes établies par le CEPD pour les institutions.

Le CEPD a effectué un contrôle préalable d'un dossier particulier concernant le traitement des données relatives à la santé par le **système d'aide à la sécurité** du Parlement européen (dossier 2009-225). La collecte de données dans ce système sert à fournir une aide aux missions en dehors des trois lieux de travail du PE en cas d'urgences médicales. Les informations sont fournies par les personnes concernées sur base volontaire et les données ne sont utilisées qu'en situation d'urgence et sont uniquement communiquées au personnel médical local si cela s'avère nécessaire.

Le CEPD a admis que le traitement des données relatives à la santé pouvait se baser sur le consentement des personnes concernées conformément à l'article 5, point d), et à l'article 10, paragraphe 2, point a), du règlement. Même si le CEPD a souligné que dans le contexte de l'emploi, l'utilisation du «consentement» en tant que base juridique était soumise à certaines restrictions, dans le cas qui nous occupe, la personne concernée est libre de fournir les catégories de données mentionnées plus haut et est informée des conséquences éventuelles de la non-communication des informations.

Le traitement des données à caractère personnel par les **crèches interinstitutionnelles** (dossier 2009-088) et par la garderie et le centre d'études à Luxembourg (dossier 2009-089) a soulevé certaines questions particulières en matière

Les institutions et organes de l'UE collectent et traitent des données relatives à la santé.

de protection des données médicales. Dans le cas du traitement par les crèches à Bruxelles, le CEPD a en particulier critiqué le fait que le traitement des données médicales dépassait le cadre de la vérification des admissions aux crèches et de la réaction en cas d'urgence et créait un suivi médical de facto des enfants par le service médical de la Commission.

Le CEPD a recommandé que le suivi de la santé et de la croissance des enfants par les crèches ou autres garderies ne puisse être effectué par le service médical que sur une base volontaire, avec le consentement explicite des parents.

Le CEPD a également critiqué la durée de trente ans pour la conservation des dossiers médicaux des enfants inscrits aux crèches à Bruxelles, durée adoptée par la Commission. Les critiques sont identiques concernant les garderies et le centre d'études à Luxembourg, où les données médicales sont conservées pendant dix ans avant d'être archivées. Le CEPD a recommandé de revoir ces périodes de conservation sur la base de la nécessité spécifique des données et des dossiers. Le CEPD a en outre recommandé que les parents puissent transférer le dossier médical de leur enfant à leur médecin lorsque leur enfant quitte la crèche.

En outre, dans les deux cas, le CEPD a estimé qu'il était essentiel que le personnel des crèches/garderies/centre d'études qui a accès à certaines données médicales concernant les enfants soit soumis au secret médical.

Évaluation du personnel

L'évaluation du personnel représente une grande part des opérations de traitement soumises au CEPD pour contrôle préalable, nombre d'entre elles concernant des procédures d'essai, d'évaluation et de promotion (voir graphique plus haut).

Les avis du CEPD en matière d'évaluation du personnel portaient souvent sur les **périodes de conservation** des données à caractère personnel après l'évaluation.

Le CEPD a estimé que les **rapports d'évaluation** ne devaient être conservés que pendant cinq ans après la fin de l'évaluation, sauf en cas de procédure juridique en cours. Toute décision découlant de ces évaluations doit être conservée dans le dossier personnel du membre du personnel concerné.

Le CEPD a également conclu, dans ces dossiers, que le **droit de rectification** accordé aux personnes concernées par l'article 14 du règlement pourrait signifier que ces personnes auraient la possibilité de demander l'insertion d'une décision d'un tribunal ou d'un autre organe en cas de révision de la décision d'évaluation ou de promotion.

Un exemple particulièrement intéressant dans le domaine de l'évaluation est l'avis du CEPD sur **l'évaluation à 360 degrés de l'intelligence émotionnelle** par l'École européenne d'administration (EEA) à l'intention de la Commission européenne (dossier 2009-100).

L'objectif de la procédure est de permettre aux participants aux formations de l'École européenne d'administration d'obtenir des commentaires et réactions, sous forme de rapport, afin de les aider à améliorer leurs compétences dans les domaines de la gestion de soi, de la gestion des relations et de la communication. L'exercice est conduit grâce à l'utilisation d'un outil en ligne: «Emotional IntelligenceView 360». Un rapport est généré automatiquement sur la base des réponses fournies par les participants et leurs collègues et n'indique pas la manière dont les collègues ont complété les réponses.

Même si l'EEA n'a pas accès aux données traitées par le contractant, ce dernier doit agir en suivant les instructions données par l'EEA. Le CEPD a donc estimé que l'EEA était le responsable du traitement des données, car c'est elle qui définit les objectifs et les moyens utilisés (utilisation de l'outil en ligne). Le contractant n'est donc pas autorisé à effectuer d'autres activités de traitement des données allant au-delà de ce qui est déterminé par l'EEA et spécifié dans le contrat.

Le CEPD a recommandé que l'EEA examine les possibilités de rendre anonyme l'utilisation de cet outil. À cet égard, il faudra tenir compte de variables telles que les mises au point informatiques, les procédures et le coût.

La question des **«notes de travail»** qui peuvent être prises lors d'une réunion d'évaluation par le notateur a également été analysée par le CEPD (dossier 2007-0421). Selon lui, ces notes sont prises par les notateurs dans leur fonction officielle et relèvent donc du champ d'application du

L'évaluation du personnel représente une partie significative des opérations de traitement soumises au CEPD en vue d'un contrôle préalable.

règlement. Même s'il n'est pas illicite de prendre des notes durant la procédure d'évaluation, il est particulièrement important que ces «notes personnelles» ne tombent pas dans une zone d'ombre et échappent ainsi à la nécessaire garantie de protection des données.

Le CEPD a estimé que les notes personnelles prises par le notateur (et par l'évaluateur) durant les entretiens devraient être détruites dès que le rapport d'évaluation est rédigé.

Recrutement

À la fin de 2008, le CEPD a publié des orientations sur le traitement des données à caractère personnel dans les procédures de recrutement en vue de la notification des opérations de traitement en la matière par les agences de l'UE (voir «2.7 Lignes directrices thématiques»).

Les procédures de recrutement spécifiques au Parlement européen ont été examinées par le CEPD, notamment le traitement des données à caractère personnel dans le cadre des **auditions des commissaires désignés** (dossier 2009-332) et de la **sélection d'un directeur pour l'Institut européen pour l'égalité entre les hommes et les femmes (EIGE)** (dossier 2008-785). Dans ces deux procédures, les données ont initialement été collectées par la Commission européenne pour être transmises au Parlement, qui a procédé à une audition des candidats. Le CEPD a accordé une attention particulière aux informations fournies aux candidats par la Commission européenne lors de la collecte des données des candidats.

Des recommandations ont également été formulées concernant la conservation des données à caractère personnel à des fins d'archivage. Même si aucun problème n'a été décelé dans les procédures de sélection spécifiques en cours d'examen, les avis sur le contrôle préalable ont montré une absence de procédure de sélection et de vérification appropriée sur la base de critères déterminés au niveau international, pour ne conserver que des données d'intérêt historique. Le CEPD a également émis des recommandations dans le domaine des mesures de sécurité.

Outils de contrôle des performances

La **centrale de données de la DG ENTR (EDW)** est un système qui permet de retrouver des données à partir de sources multiples afin de procéder à leur traitement et leur recoupement dans le but d'obtenir des éléments de mesure, des indicateurs et des rapports sur les activités de la DG ENTR au sein de la Commission européenne (dossier 2008-487). Sur la base des informations compilées, la DG ENTR établira des rapports de mesure des performances destinés aux chefs d'unité, aux directeurs et au directeur général. Le système n'est pas conçu pour mesurer les performances individuelles des membres du personnel, mais pour évaluer les performances de la direction générale dans son ensemble. À cet égard, le CEPD a souligné que l'utilisation des données devait se limiter à l'usage spécifique mentionné dans la notification, par exemple l'élaboration d'un tableau de bord de gestion et la mise en évidence de divergences avec les données émanant de différentes sources.

Le CEPD a souligné que cette agrégation de bases de données accroissait le risque de **«détournement d'usage»** lorsque l'interconnexion de deux bases de données (ou plus) conçues pour des finalités distinctes débouche sur une troisième pour laquelle ces deux bases n'ont pas été créées. Or, ce résultat est tout à fait contraire au principe de limitation de la finalité. Pour être autorisée, une telle finalité doit être clairement limitée et la preuve de sa nécessité doit être apportée. L'EDW devrait donc se limiter à l'utilisation des données provenant des bases de données déclarées dans la notification et nécessiter une autorisation supplémentaire si d'autres bases de données devaient elles aussi servir de source.

Gestion du temps

Les systèmes de gestion du temps (TIM) ont continué à revêtir un intérêt particulier, surtout lorsque les institutions et organes de l'UE décident de **combiner les systèmes de gestion du temps** à d'autres systèmes.

La Cour des comptes entendait relier son système de vérification de la gestion des ressources humaines (Assyst) à son système d'horaire flexible (Efficient) par l'intermédiaire de l'**interface ART** (dossier 2008-239). La finalité de l'opération de traitement est de permettre aux auditeurs et leurs

chefs d'unité de mettre en concordance les temps enregistrés dans Assyst avec Efficient, de garantir leur correspondance et de contrôler les divergences.

Le CEPD a conclu que comme l'agrégation de bases de données augmentait le risque de «détournement d'usage», cette finalité devait être clairement limitée et la nécessité devait en être démontrée. Dans ce cas précis, la nécessité n'était pas clairement établie dès le départ et devait donc être développée plus avant. Cet instrument a depuis lors été adopté par la Cour des comptes.

Des réserves ont également été émises par le CEPD dans son avis sur le système envisagé **de vérification des pointages flexitime par rapport aux données sur l'accès physique** à l'intention du secrétariat général du Conseil (SGC) (dossier 2009-477). Le SGC utilise un système flexitime qui gère le temps de travail et les présences, facilitant ainsi le calcul des heures supplémentaires et des droits à congés. Cette application a déjà fait l'objet d'un contrôle préalable par le CEPD. Le SGC dispose également d'un système de contrôle d'accès géré par le Bureau de sécurité accessible aux services de l'administration dans le cadre d'une enquête administrative formelle. La comparaison des données recueillies par les deux systèmes vise à identifier les personnes qui ne respectent pas les règles flexitime et à évaluer leur comportement. Le système pourrait également conduire à l'adoption de mesures disciplinaires.

La gestion du temps peut soulever des problèmes en matière de protection des données, en particulier lorsque les institutions de l'UE décident d'interfacer les systèmes de gestion du temps avec d'autres systèmes.

Dans son avis, le CEPD a estimé que la nécessité et la proportionnalité de la vérification des pointages flexitime par rapport aux données sur le contrôle d'accès physique étaient sujettes à caution. Selon le CEPD, aucune preuve raisonnable ne démontre que la mise en œuvre d'un système de contrôle comparant les pointages aux données sur le contrôle de l'accès physique est nécessaire à des fins de gestion du personnel ou de fonctionnement du SGC.

Le CEPD a donc estimé que le processus envisagé violerait le règlement à différents niveaux (nécessité et proportionnalité, changement de finalité, qualité des données) sauf s'il était mené dans le cadre d'une enquête administrative spécifique.

Enquêtes de sécurité

Le CEPD a analysé les procédures mises en place pour traiter les menaces vis-à-vis des intérêts de la Commission dans les domaines du **contre-espionnage** et du **contre-terrorisme** (dossier 2008-440). Deux traitements spécifiques ont été examinés: les **enquêtes de sécurité** et les **procédures de screening.** Les enquêtes de sécurité portent sur les fuites d'informations classifiées de l'UE émanant d'un travailleur de la Commission tandis que les procédures de screening visent à empêcher le recrutement ou la conclusion d'un contrat avec des personnes représentant une menace pour les intérêts de la Commission.

Le CEPD a salué les différentes mesures mises en place par l'unité responsable, en particulier le fait que l'unité évalue en priorité, au cas par cas, la **nécessité** de la procédure de screening sur la base de critères précis. Le CEPD a recommandé que les enquêteurs gardent à l'esprit les critères de **proportionnalité** lorsqu'ils collectent et traitent des données à caractère personnel.

Enregistrements sonores

L'enregistrement sonore des appels téléphoniques soulève des inquiétudes particulières car il viole le ***principe de confidentialité des communications.***

Le CEPD a étudié l'examen de l'enregistrement des communications à des fins de sécurité à l'Institut de l'énergie du Centre commun de recherche (CCR-IE)

(dossier 2008-0014). Ce dossier portait sur l'enregistrement des appels entrants et sortants (y compris les détails sur le numéro d'origine et de destination, ainsi que la date, l'heure et la durée de l'appel) à utiliser en cas d'incidents opérationnels, d'urgence, d'évaluation des exercices d'urgence et d'enquêtes sur les menaces potentielles. Le CEPD a certifié que l'enregistrement des appels téléphoniques était licite au regard de la législation nationale sur les installations nucléaires, mais a recommandé que les personnes extérieures qui contactent le standard soient informées du fait que leur communication sera enregistrée à des fins de sécurité au début de l'appel.

EudraVigilance

L'Agence européenne des médicaments (EMA) est responsable de la base de données EudraVigilance, qui contient des **rapports sur les effets indésirables présumés des médicaments à usage humain** (rapports de sécurité concernant des cas particuliers, ou rapports de sécurité). EudraVigilance facilite la notification et l'évaluation de ces rapports. Les autorités nationales compétentes, les titulaires d'autorisation de mise sur le marché et les promoteurs d'essais cliniques fournissent ces informations à l'EMA.

Le CEPD a analysé le traitement des données via EudraVigilance et souligné la responsabilité partagée des différents responsables du traitement des données pour garantir le respect des droits des personnes concernées (dossier 2008-402). Les responsables du traitement des données aux niveaux national et européen doivent coordonner et unir leurs efforts pour garantir le respect des législations nationales et européennes en matière de protection des données.

Le CEPD a recommandé à l'EMA d'examiner la possibilité d'anonymiser ou de pseudo-anonymiser les informations à caractère personnel dans les rapports de sécurité concernant des cas particuliers, et de réduire au minimum les données à caractère personnel dans ces rapports. Il a également recommandé que l'EMA, en collaboration avec les responsables nationaux du traitement des données, élabore un projet de note type qui donnerait aux particuliers les informations requises et qui devrait mentionner EudraVigilance.

Levée de l'immunité

Le protocole sur les privilèges et immunités des Communautés européennes établit un certain nombre d'immunités au profit des fonctionnaires et autres agents des Communautés. L'**Office d'investigation et de discipline** de la Commission (IDOC) est chargé d'évaluer les demandes de levée de ces immunités émanant des tribunaux nationaux ou d'autres organes nationaux. Le CEPD a procédé à un contrôle préalable de la procédure mise en place par l'IDOC pour la levée de ces immunités (dossier 2008-645).

La plupart du temps, les autorités nationales demandent à l'IDOC de mener son enquête dans le secret, ce qui limite les droits des personnes concernées car elles ne sont pas informées de l'enquête et ne peuvent exercer leurs droits d'accès et de rectification au cours de ces enquêtes. Le CEPD a souligné que toute restriction des droits des personnes concernées devait être temporaire et que les personnes concernées devaient être en mesure d'exercer leur droit d'accès dès que le secret ne se justifiait plus.

À l'issue de l'enquête, l'IDOC soumet sa décision et certaines données au tribunal demandeur ou à l'autorité nationale demanderesse. Le CEPD a recommandé que l'IDOC dresse une liste des destinataires des données, enregistrant la justification légale des transferts.

Étant donné que la levée de l'immunité s'inscrit généralement dans le cadre d'une procédure plus large qui peut — ou non — conduire à d'autres actions, le CEPD a recommandé de réduire les durées de conservation des dossiers lorsque les procédures disciplinaires ou judiciaires sont abandonnées ou que la personne concernée est acquittée.

Projets pilotes

Dans trois dossiers portant sur des projets pilotes, le CEPD a profité de l'occasion pour rappeler aux institutions et aux agences les **règles relatives au contrôle préalable des projets pilotes.** En fournissant des recommandations avant la mise en place complète d'un système, le CEPD veut réduire au minimum les modifications ultérieures effectuées par le responsable du traitement des données.

Les résultats du projet pilote doivent être analysés et communiqués au CEPD **avant** le lancement du projet général et le CEPD doit être informé de toute modification susceptible d'avoir un impact sur le traitement de données à caractère personnel. L'avis rendu sur le contrôle préalable devrait être considéré comme la conclusion de l'analyse complète du projet pilote.

2.3.4. Consultations quant à la nécessité d'un contrôle préalable

Au cours de l'année 2009, le CEPD a reçu 21 consultations des DPD sur la nécessité d'un contrôle préalable (sur la base de l'article 27, paragraphe 3, du règlement), dont 11 émanant du DPD du Parlement européen.

*Plusieurs dossiers ont été déclarés **soumis au contrôle préalable,** par exemple:*

- *les données relatives aux grèves à la Banque centrale européenne;*
- *les auditions des commissaires désignés au Parlement européen;*
- *l'évaluation ergonomique des environnements de travail au Parlement européen;*
- *la nomination des fonctionnaires aux postes élevés au Parlement européen.*

Le traitement des données par le **service juridique et l'unité affaires juridiques du Parlement européen** dans le cadre de leurs missions respectives d'examen des dossiers, de préparation des demandes et des réclamations et de procédures juridiques n'a pas été considéré comme devant être soumis au contrôle préalable du CEPD (dossier 2009-263).

La simple présence éventuelle de **données sensibles** ne signifie pas automatiquement qu'un contrôle préalable est nécessaire. Toutefois, la présence dans des dossiers de données sensibles telles que des données relatives à la santé ou aux infractions signifie qu'il convient d'accorder une attention particulière à l'adoption de mesures de sécurité conformément à l'article 22 du règlement.

Même si certaines opérations de traitement pourraient être liées à une évaluation d'éléments personnels, le traitement ne vise pas à évaluer la personne concernée et l'article 27, paragraphe 2, point b), ne s'applique pas.

De la même manière, en ce qui concerne l'article 27, paragraphe 2, point d), même si les opérations de traitement peuvent avoir pour conséquence pour un individu la privation d'un droit, d'une prestation ou d'un marché, ce n'est pas leur finalité unique et spécifique.

Le CEPD a également été consulté sur le traitement des données à caractère personnel dans le cadre de la **procédure de sélection des assistants parlementaires.** D'après les informations reçues, la procédure de sélection n'est pas effectuée par le PE, et le CEPD a dès lors estimé que le traitement ne pouvait être soumis à un contrôle préalable. Le CEPD a néanmoins souligné que cela ne signifiait pas que les assistants parlementaires ne jouissaient pas de certains droits de protection des données garantis par le Parlement européen.

2.3.5. Notifications non soumises au contrôle préalable ou retirées

En 2009, le CEPD a également examiné 21 dossiers pour lesquels il a conclu qu'ils n'étaient pas soumis au contrôle préalable. Dans ces situations, le CEPD peut tout de même émettre des recommandations.

Youthlink 2

Un dossier intéressant était celui de **«Youthlink 2»,** le principal dépôt de données (statistiques et financières) relatives aux projets et activités présentés au titre du programme «Jeunesse en action» à la Commission européenne (dossier 2008-484).

Le CEPD a conclu, sur la base des faits communiqués, que la sélection des bénéficiaires au titre des programmes «Jeunesse en action» **ne reposait pas sur une évaluation des compétences ou du comportement individuels,** mais sur un contrôle du projet proposé selon des critères préétablis ainsi qu'un contrôle des capacités financières et opérationnelles des entités juridiques ou groupes qui ont présenté une demande. En outre, l'évaluation en question est effectuée de manière décentralisée, non par le responsable du traitement au sein de la Commission européenne, mais par les agences nationales sous réserve de la législation en matière de protection des données qui leur est applicable, ou par l'Agence exécutive «Éducation, audiovisuel et culture» (EACEA). Pour ces raisons, le CEPD a estimé que l'article 27, paragraphe 2, point b), du règlement n'était pas applicable en l'espèce.

Enquête sur la satisfaction des clients

Le CEPD a estimé que les **«enquêtes sur la satisfaction des clients»** réalisées à la Banque centrale européenne **ne devaient pas faire l'objet d'un contrôle préalable,** étant donné que ces enquêtes ne visent pas à évaluer des personnes, mais plutôt des services, de la même façon grosso modo qu'un audit vise à évaluer la conformité du travail accompli par une unité organisationnelle ou du fonctionnement d'un processus, plutôt que le travail réalisé par des personnes (dossier 2008-780). La BCE s'est efforcée de réduire le plus possible le risque que certaines informations personnelles soient incluses dans les résultats des enquêtes, en particulier les résultats tirés de réponses données à des questions ouvertes.

Utilisation des téléphones portables

Après avoir reçu la notification sur l'**utilisation des téléphones portables** par le personnel de l'Agence exécutive pour la compétitivité et l'innovation (EACI) se rendant en mission, le CEPD a conclu que ce dossier **n'était pas soumis au contrôle préalable** (dossier 2009-162). Le traitement avait pour objet de faire en sorte que les coûts des appels à caractère privé soient remboursés à l'EACI. L'évaluation de la compétence, du rendement ou du comportement des membres du personnel ne faisant pas partie des attributions du traitement, il ne tombait donc pas sous le coup de l'article 27, paragraphe 2, point b).

Gestion de l'identité et de l'accès

Le CEPD a également estimé que le **système de gestion de l'identité et de l'accès** de la Cour des comptes ne devait pas être soumis au contrôle préalable (dossier 2009-639). Même si le système utilise certaines informations (nom, prénom, date de naissance) pour créer les comptes utilisateurs et donner accès à ces comptes, il n'«évalue» pas les personnes, mais authentifie plutôt leur identité et leurs droits d'accès. Le simple contrôle des droits sur la base de règles prédéfinies n'entraîne donc aucune évaluation de fait de l'efficacité, des compétences, de la capacité de travailler ou du comportement de l'utilisateur et n'est donc pas couvert par l'article 27, paragraphe 2, point b).

2.3.6. Suivi des avis relatifs aux contrôles préalables

*Un avis relatif au contrôle préalable remis par le CEPD comprend des **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 lorsque 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 du règlement (CE) n° 45/2001. Il peut en particulier saisir l'institution ou l'organe de l'UE concerné.*

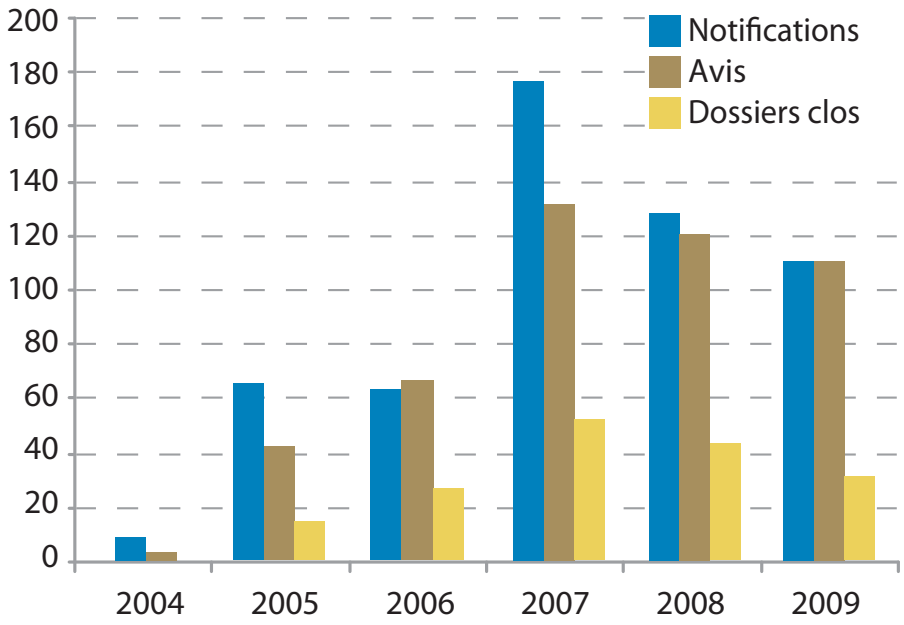
La plupart des dossiers de contrôle préalable ont débouché sur des recommandations, concernant principalement les sujets suivants:

- information des personnes concernées;
- durée de conservation des données;
- limitation de la finalité;
- droits d'accès et rectification.

Les institutions et organes sont disposés à suivre ces recommandations et, à ce jour, il n'a pas été nécessaire de prendre des décisions assorties d'un impératif d'exécution. 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.

Malgré les rappels aux institutions et organes pour qu'ils transmettent ces informations, en 2009, le CEPD n'a clos que 32 dossiers, laissant un grand nombre de dossiers ouverts. Le CEPD a dès lors invité les institutions et organes à assurer le suivi de ses avis de manière qu'il puisse clore les dossiers.

Situation comparative



2.3.7. Conclusions et perspectives

La plupart des institutions principales atteignent la fin du processus de notification de leurs opérations de traitement existantes et la plupart des agences progressent dans la notification de leurs activités principales impliquant le traitement de données à caractère personnel et les procédures administratives standard (conformément à la nouvelle procédure établie pour les agences).

Les 110 avis adoptés ont permis au CEPD de bien appréhender les opérations de traitement au sein des administrations européennes et lui ont permis de souligner ses recommandations. L'expérience acquise dans l'application du règlement lui a également permis d'obtenir une certaine expertise et de fournir des orientations générales dans certains domaines (voir «2.7 Lignes directrices thématiques»).

La plupart des dossiers de contrôle préalable ont débouché sur des recommandations du CEPD et requièrent un retour d'informations des institutions et organes sur la manière dont ces recommandations ont été mises en œuvre. Peu de dossiers ont été refermés en 2009 et le CEPD continuera donc d'insister pour que des avancées aient lieu dans ce domaine.

2.4. Réclamations

2.4.1. Les fonctions du CEPD

L'une des fonctions principales du CEPD est définie par l'article 46 du règlement (CE) n° 45/2001: le CEPD «entend et examine les réclamations» et «effectue des enquêtes, soit de sa propre initiative, soit sur la base d'une réclamation».

En principe, une personne ne peut présenter une réclamation que pour une violation présumée de ses droits en matière de protection des données à caractère personnel. Seul le personnel de l'UE peut se plaindre d'une violation présumée des règles en matière de protection des données, que le plaignant soit directement touché par le traitement ou pas. Le statut des fonctionnaires de l'Union européenne permet également de soumettre une réclamation au CEPD (article 90 *ter*).

Dans un dossier intéressant concernant les **données d'un mineur,** le CEPD a estimé que les données relatives à un enfant pouvaient, en principe, être consultées par un parent qui exerce son autorité parentale légitime. Le dossier portait sur l'accès aux documents relatifs à l'inscription d'un enfant à une crèche gérée par une institution de l'UE. Le plaignant affirmait qu'il n'avait pas obtenu un accès total aux documents soumis par l'autre parent,

Toute personne peut se plaindre auprès du CEPD concernant le traitement de données à caractère personnel par l'administration de l'UE.

dont il était divorcé. En particulier, le nom des personnes autorisées à aller chercher l'enfant à la crèche était partiellement mentionné.

Le CEPD a affirmé qu'en principe, le parent qui exerce son autorité parentale conjointe légitime a le droit d'avoir accès aux données de son enfant. Dans ce dossier, il a conclu que ces droits couvraient également les données des tierces personnes autorisées à venir chercher l'enfant, puisque ces données étaient par nature connectées à celles de l'enfant.

Le CEPD a estimé qu'en refusant de donner au plaignant l'accès aux données de son enfant de manière intelligible, l'institution en question violait l'article 13 du règlement.

Le règlement prévoit que le CEPD peut uniquement traiter des réclamations soumises par des **personnes physiques.** Les réclamations soumises par des entreprises ou des personnes morales ne sont pas recevables. Les plaignants doivent également s'identifier et les requêtes anonymes ne sont donc pas considérées comme des «réclamations». Toutefois, les informations anonymes peuvent être prises en considération dans le cadre d'une autre procédure (enquête d'initiative ou demande de notification d'une opération de traitement de données, etc.).

Une réclamation devant le CEPD ne peut porter que sur le traitement de données à caractère personnel. *Le CEPD n'est pas compétent pour traiter les cas de mauvaise administration, pour modifier le contenu des documents que le plaignant souhaite contester ou pour octroyer des dommages et intérêts.*

En particulier, le fait que le règlement parle de «rectification des données à caractère personnel» ne signifie pas que le CEPD est compétent pour réviser les décisions sur le fond parce qu'elles contiennent certaines données à caractère personnel. Pour ce type de réclamations, il est conseillé au plaignant de s'adresser au Médiateur européen ou à la juridiction compétente.

Le traitement de données à caractère personnel faisant l'objet d'une réclamation doit avoir été effectué par ***un des organes ou institutions de l'UE****. En outre, le CEPD n'est pas une instance de recours pour les décisions prises par les autorités nationales chargées de la protection des données.*

2.4.2. Procédure de traitement des réclamations

Le CEPD examine les réclamations en vertu de la base juridique en vigueur, des principes généraux du droit européen et des bonnes pratiques administratives communes aux institutions et organes de l'UE. Pour faciliter le traitement des réclamations, en décembre 2009, le CEPD a adopté un **manuel interne** destiné à fournir des orientations à son personnel en matière de traitement des réclamations. En particulier, le CEPD a procédé à un examen approfondi des conditions de recevabilité des réclamations. En 2009, le CEPD a également mis en place un **outil statistique** conçu pour examiner les activités liées aux réclamations, et en particulier pour suivre l'évolution de dossiers particuliers.

À tous les stades du traitement de la réclamation, le CEPD respecte les principes de proportionnalité et d'équité. Guidé également par les principes de transparence et de non-discrimination, il prend les mesures appropriées en tenant compte:

- de la nature et de la gravité de la violation alléguée des règles régissant la protection des données;
- de l'importance du préjudice qu'une ou plusieurs personnes ont ou peuvent avoir subi du fait de la violation;
- de l'importance potentielle de l'affaire, en tenant compte des autres intérêts publics et/ou privés en cause;
- de la probabilité d'établir l'existence de la violation;
- de la date exacte des événements en cause, de tout comportement ne produisant plus d'effets, de l'élimination de ces effets ou d'une garantie satisfaisante quant à l'élimination de ces effets.

Le CEPD examine attentivement chaque réclamation qu'il reçoit. L'examen préliminaire est spécifiquement destiné à vérifier si la réclamation remplit les conditions d'ouverture d'une enquête et s'il existe des éléments suffisants pour justifier l'ouverture d'une enquête.

Une réclamation pour laquelle le CEPD **n'a pas de compétence juridique** sera déclarée irrecevable et le plaignant en sera informé. Dans ce cas, le CEPD indique au plaignant les autres organes compétents (par exemple tribunal, Médiateur, autorité nationale de protection des données, etc.).

Une réclamation portant sur des faits **manifestement insignifiants** ou des questions dont l'examen nécessiterait des **efforts disproportionnés** ne fera pas l'objet d'une enquête complémentaire. Le CEPD ne peut examiner que les réclamations qui concernent une violation **réelle ou potentielle,** et pas simplement hypothétique, des règles régissant le traitement des données à caractère personnel. Il s'agit notamment d'analyser quelles sont les autres options disponibles pour traiter de la question, que ce soit pour le plaignant ou le CEPD. Celui-ci peut par exemple ouvrir une enquête d'initiative sur un problème général au lieu d'ouvrir une enquête sur un dossier individuel soumis par le plaignant. Dans ce cas, le plaignant est informé de ces autres moyens d'action.

*Le CEPD a été informé anonymement du fait que les données à caractère personnel des candidats qui passent les **tests de présélection** des concours de fonctionnaires européens sont traitées par un **sous-traitant extérieur situé dans un État hors UE.** Le CEPD a ouvert une enquête en la matière de sa propre initiative et est arrivé à la conclusion qu'en réalité, même si l'Office européen de sélection du personnel avait conclu un contrat avec une entreprise extérieure enregistrée au Royaume-Uni, les opérations de traitement des données étaient effectuées aux États-Unis. Le CEPD a demandé à l'EPSO de vérifier si toutes les conditions fixées à l'article 9 du règlement étaient respectées et de modifier le contrat afin d'y inclure des garanties supplémentaires pour les personnes concernées.*

La réclamation est en principe irrecevable si le plaignant n'a pas d'abord contacté l'institution concernée pour qu'elle remédie à la situation. Si le plaignant n'a pas contacté l'institution, il doit fournir au CEPD des raisons suffisantes pour expliquer cette inaction.

Si la question est déjà examinée par des organes administratifs — par exemple si une enquête interne par l'institution concernée est en cours —, la réclamation est en principe irrecevable. Toutefois, le CEPD peut décider, sur la base des éléments

particuliers du dossier, d'attendre l'issue de ces procédures administratives avant de commencer son enquête. À l'inverse, si la même question (ou les mêmes circonstances factuelles) fait déjà l'objet d'un examen par un tribunal, la réclamation est déclarée irrecevable.

Pour assurer le traitement cohérent des réclamations concernant la protection des données et éviter toute redondance, le Médiateur européen et le CEPD ont signé un mémorandum d'accord en novembre 2006 qui stipule entre autres qu'une réclamation qui a déjà été déposée ne peut être ouverte une seconde fois par l'autre institution, sauf si des éléments nouveaux importants sont apportés.

En ce qui concerne les **délais,** si les faits sont communiqués au CEPD après plus de deux ans, la réclamation est en principe irrecevable. La période de deux ans commence le jour où le plaignant a pris connaissance des faits.

Lorsqu'une réclamation est recevable, le CEPD procède à une **enquête** aussi approfondie qu'il l'estime utile. Cette enquête peut comprendre une demande d'information à l'institution concernée, une révision des documents concernés, une rencontre avec le responsable du traitement, une enquête sur place, etc. Le CEPD a le pouvoir d'obtenir l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires pour l'enquête de la part de l'institution ou de l'organe concerné. Il peut également avoir accès à tous les locaux dans lesquels un responsable du traitement, une institution ou un organe exerce ses activités.

À la fin de l'enquête, il transmet sa **décision** au plaignant ainsi qu'au responsable du traitement des données. Dans cette décision, il exprime sa position concernant toute violation des règles régissant la protection des données par l'institution concernée. Le CEPD **dispose de vastes pouvoirs,** allant du simple conseil aux personnes concernées à l'interdiction du traitement ou la saisine de la Cour de justice de l'Union européenne, en passant par un avertissement ou une admonestation au responsable du traitement.

Toute partie intéressée peut demander au CEPD de revoir sa décision dans un délai d'un mois à compter de la date d'adoption de cette décision. Les parties concernées peuvent également former un recours directement auprès de la Cour de justice. À deux reprises en 2009, les plaignants ont contesté les décisions du CEPD auprès du Tribunal de première instance (affaires T-164/09 et T-193/09).

2.4.3. Confidentialité garantie pour les plaignants

*Le CEPD reconnaît que certains plaignants prennent des risques pour leur carrière en dévoilant des violations des règles de protection des données et que la **confidentialité** doit donc être garantie aux plaignants et informateurs qui le demandent. D'autre part, le CEPD s'est engagé à travailler **de manière transparente** et à publier au moins le fond de ses décisions. Les procédures internes du CEPD reflètent ce difficile équilibre.*

Généralement, les réclamations sont traitées de manière confidentielle. Le **traitement confidentiel** signifie que les informations personnelles ne sont pas divulguées à des personnes extérieures au CEPD. Toutefois, pour le déroulement correct de l'enquête, il pourrait s'avérer nécessaire d'informer les services de l'institution concernée et les tierces parties impliquées du contenu et de l'identité du plaignant. Le CEPD envoie également une copie de sa correspondance avec l'institution au délégué à la protection des données de ladite institution.

Si le plaignant exige l'**anonymat** envers l'institution, le DPD ou les tierces personnes concernées, il est invité à en expliquer les raisons. Le CEPD analyse ensuite ses arguments et examine les conséquences pour la viabilité de son enquête future. S'il décide de ne pas accepter l'anonymat du plaignant, il explique pourquoi et demande au plaignant s'il accepte que le CEPD examine la réclamation sans garantir l'anonymat ou s'il préfère retirer sa réclamation, auquel cas l'institution concernée ne sera pas informée de son existence. Dans ce cas, le CEPD peut mener d'autres actions en la matière, sans révéler à l'institution concernée l'existence de la réclamation. Il s'agit alors d'une enquête d'initiative ou d'une demande de notification d'une opération de traitement des données.

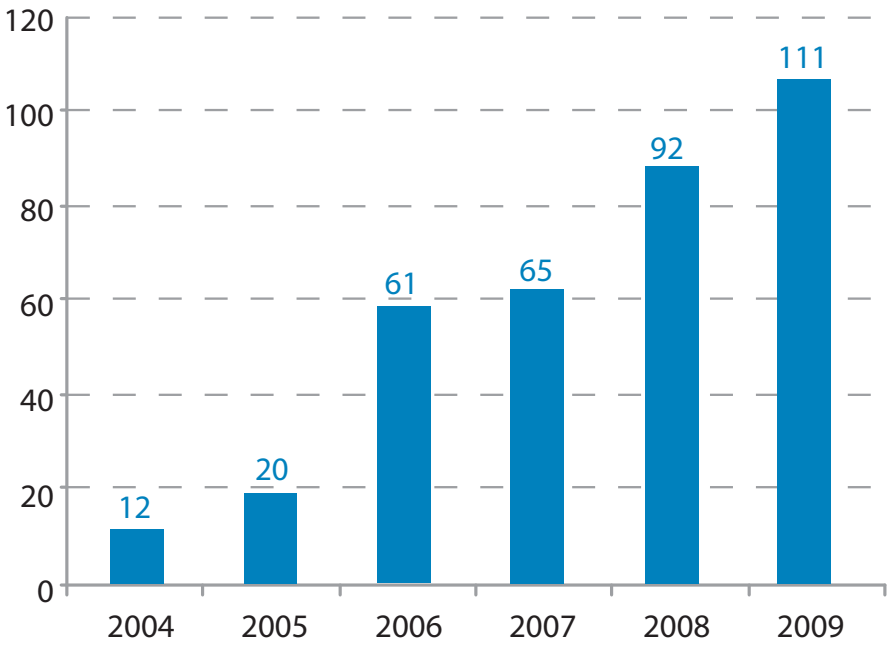
À l'issue d'une enquête, tous les **documents relatifs à la réclamation,** y compris la décision finale, restent en principe confidentiels. Ils ne sont pas entièrement publiés ni transmis à des tiers. Toutefois, un résumé anonyme de la réclamation peut être publié par le CEPD sur son site internet et dans son rapport annuel sous une forme qui ne permet d'identifier ni le plaignant ni les tiers. Le CEPD peut également décider de publier la décision finale in extenso s'il

s'agit de dossiers importants. Il doit alors prendre en considération la demande de confidentialité du plaignant et ne permettra donc pas d'identifier le plaignant ou les autres personnes concernées.

2.4.4. Réclamations traitées en 2009

2.4.4.1. Nombre de réclamations

Nombre des réclamations reçues (évolution 2004-2009)



Le nombre des réclamations reçues par le CEPD a augmenté, et leur complexité s'est accrue. ***En 2009, le CEPD a reçu 111 réclamations*** *(hausse de 32 % par rapport à 2008), dont* ***69 ont été jugées irrecevables****, la majorité portant sur un traitement au niveau national, et pas au niveau d'une institution ou d'un organe de l'UE.*
Les 42 réclamations restantes ont nécessité une enquête approfondie (hausse de 83 % par rapport à 2008). En outre, 14 réclamations recevables soumises les années précédentes (13 en 2008 et 1 en 2007) en étaient toujours au stade de l'enquête ou de l'examen.

2.4.4.2. Nature des plaignants

Sur les 111 réclamations déposées, 26 (23 %) ont été soumises par des membres du personnel des institutions ou organes de l'UE, y compris des anciens membres et des candidats. Une réclamation était anonyme et pour les 84 autres réclamations, le plaignant ne semblait pas avoir de lien professionnel avec l'administration de l'UE.

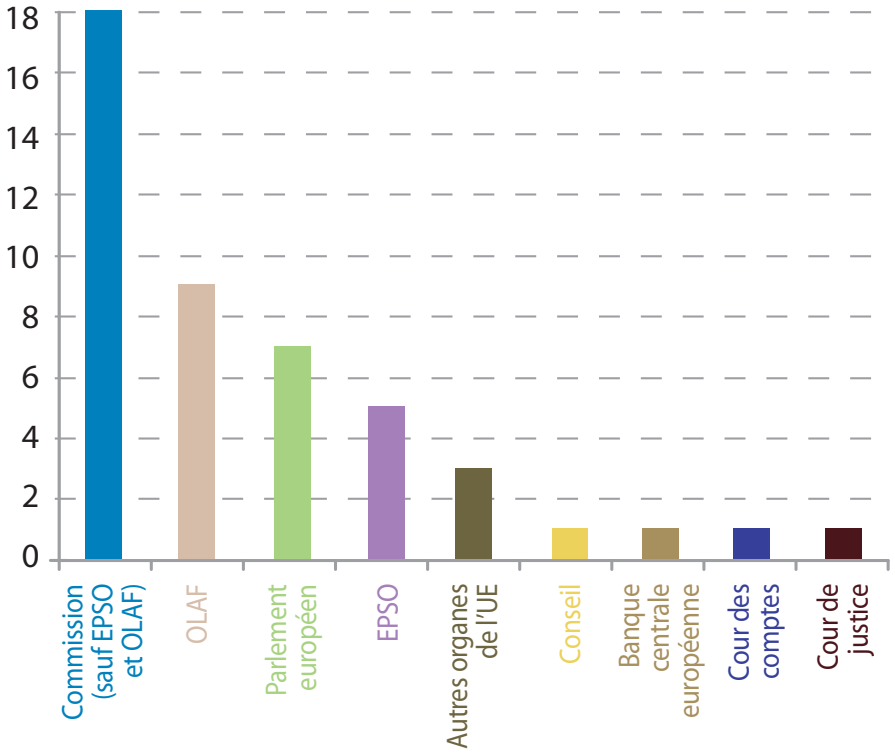
2.4.4.3. Institutions concernées par les réclamations

Sur l'ensemble des réclamations recevables reçues en 2009, la majorité (plus de 70 %) étaient dirigées contre la **Commission européenne, notamment l'OLAF et l'EPSO.** Ce n'est pas étonnant car la Commission traite plus de données à caractère personnel que les autres institutions et organes de l'UE. Le nombre élevé de réclamations concernant l'OLAF et l'EPSO peut s'expliquer par la nature des activités exercées par ces organes.

2.4.4.4. Langue des réclamations

La majorité des réclamations étaient rédigées en anglais (64 %), l'allemand (19 %) et le français (9 %) étant moins souvent utilisés. Les réclamations dans d'autres langues sont relativement rares (8 %).

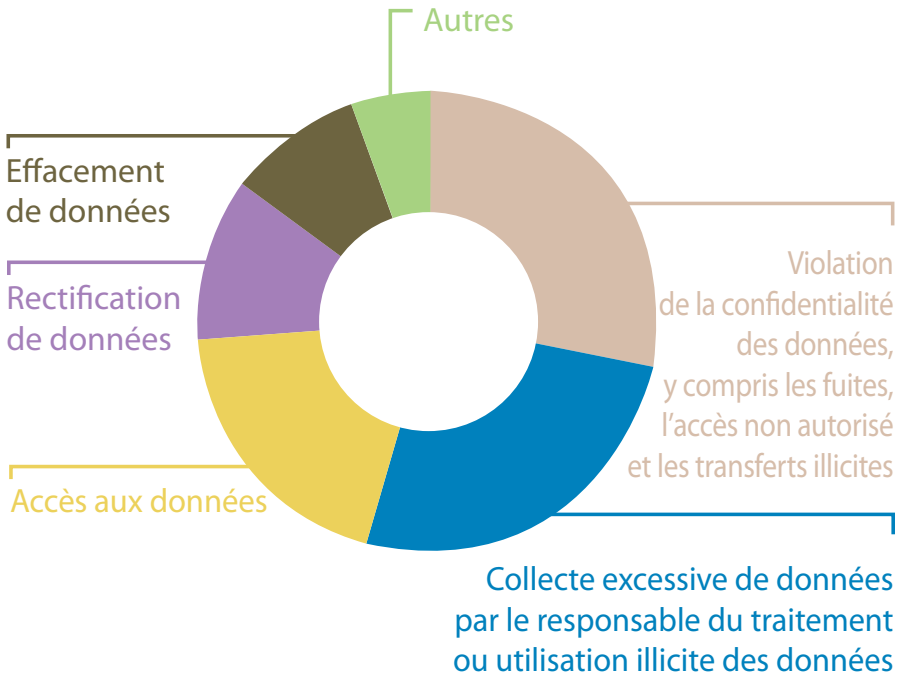
Institutions concernées



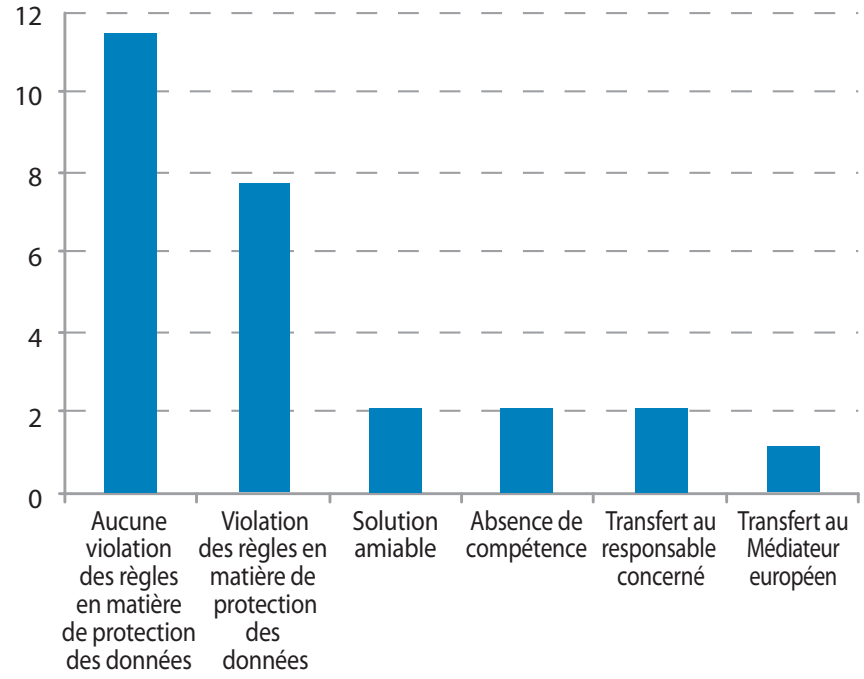
2.4.4.5. Types de violations invoqués

Les principaux types de violations aux règles de protection des données invoqués par les plaignants en 2009 ont été les suivants: violation de la confidentialité des données, notamment fuites, accès non autorisé et transferts illicites (31 %) et collecte excessive de données ou utilisation illégale des données par le responsable du traitement (28 %). Les autres types de violations ont été moins fréquents, en particulier l'accès aux données (20 %), la rectification des données (12 %), l'effacement des données (10 %), la vidéosurveillance (2 %), le transfert de données en dehors de l'UE (2 %) et la perte de données (2 %).

Types de violations invoqués



Résultats des enquêtes du CEPD



2.4.4.6. Résultats des enquêtes du CEPD

Dans 12 dossiers résolus en 2009, le CEPD n'a constaté aucune violation des règles en matière de protection des données.

Dans un dossier contre la Commission européenne, un ancien membre du personnel se plaignait du refus qui lui avait été opposé concernant la délivrance d'une copie d'un rapport concernant une enquête administrative diligentée par la Commission. Celle-ci refusait de lui donner accès au texte complet du rapport, justifiant ce refus par la nécessité de protéger les droits et libertés des autres, en particulier des personnes qui avaient témoigné dans cette affaire. Toutefois, elle lui a permis d'accéder aux constatations factuelles le concernant et aux conclusions du rapport. Vu que la divulgation du texte complet aurait effectivement pu avoir des conséquences négatives sur certaines des personnes concernées, le CEPD a estimé que la façon de procéder de la Commission avait respecté les dispositions de l'article 13 du règlement, tout en préservant les droits et libertés des autres.

À l'inverse, dans 8 dossiers, le CEPD a constaté un non-respect des règles de protection des données et a soumis des recommandations au responsable du traitement des données.

Dans un dossier, un membre du personnel se plaignait d'abus par un organe dans le cadre d'une enquête sur ses qualifications professionnelles. Il affirmait que son employeur avait illégalement transféré des documents «marqués du sceau de la confidentialité» établissant ses qualifications à plusieurs destinataires au sein et en dehors des institutions de l'UE.

Sur la base des informations fournies par le responsable du traitement des données, le CEPD a conclu que les transferts à l'intérieur de l'UE étaient nécessaires pour que les destinataires puissent légitimement exercer leurs activités. Pour ce qui est des transferts aux tierces personnes, si le CEPD était satisfait que ceux-ci aient été effectués dans le respect de l'article 8, il a estimé que le transfert à une entreprise de conseils en matière de médias (engagée pour répondre à une éventuelle couverture médiatique de l'enquête) était excessif au vu des fonctions exercées par ce destinataire. Le CEPD a donc conclu que ce transfert de données violait le principe de qualité des données et que l'organe de l'UE concerné violait en conséquence l'article 4, paragraphe 1, point c).

Dans deux dossiers, le CEPD a contribué à une solution informelle entre le plaignant et l'institution concernée et n'a signé aucune décision.

2.4.5. Autres travaux dans le domaine des réclamations

L'adoption du **manuel interne relatif au traitement des réclamations** en décembre 2009 a facilité la révision des pages concernées du site internet du CEPD. La nouvelle page décrit les principaux éléments de la procédure et comprend un formulaire téléchargeable de dépôt de réclamation ainsi que des informations sur la recevabilité. Ces informations ont été publiées sur le site internet du CEPD au début de 2010 et aideront les plaignants potentiels à déposer une réclamation. Elles devraient également limiter le nombre de réclamations manifestement irrecevables et fournir aux CEPD des informations plus complètes et pertinentes, permettant un traitement plus efficace des réclamations. Il est à espérer qu'une version interactive du formulaire de dépôt de réclamation suivra, permettant aux utilisateurs de le compléter en ligne et de l'envoyer automatiquement au CEPD.

2.5. Contrôle du respect du règlement

Le CEPD est chargé d'assurer le suivi et de veiller à l'application du règlement (CE) n° 45/2001 (article 41, paragraphe 2). Le contrôle a notamment pris la forme d'un rapport intitulé «printemps 2009». Cet exercice faisait suite à une initiative similaire («printemps 2007») et a pris la forme de lettres adressées aux institutions et organes de l'UE pour demander des informations à jour sur les progrès effectués dans certains domaines. En plus de cet exercice général de contrôle, des enquêtes ont été menées dans certaines institutions et certains organes pour vérifier leur respect du règlement sur des questions spécifiques.

2.5.1. L'exercice «printemps 2009»

À l'issue de l'exercice, le CEPD a publié un deuxième rapport général sur les progrès accomplis dans la mise en œuvre des règles et principes de protection des données par les institutions et organes de l'UE. Le rapport indique qu'en général, les institutions de l'UE ont accompli des progrès significatifs concernant le respect des exigences en matière de protection des données, même si le niveau de conformité constaté dans les agences est plus faible.

Principaux résultats dans les institutions

- **Inventaire des opérations de traitement:** le CEPD est satisfait du fait que toutes les institutions, sauf une, ont dressé un inventaire des opérations de traitement impliquant des données personnelles, ce qui permet une approche plus systématique de la mise en œuvre.
- **Notification des opérations de traitement aux DPD par les responsables du traitement:** le CEPD note une hausse du nombre d'institutions qui ont achevé le processus. À la fin de 2008, six institutions au moins pouvaient affirmer que toutes les opérations de traitement avaient été notifiées au DPD, contre seulement deux au début de 2008.
- **Notification des opérations de traitement au CEPD pour contrôle préalable:** seules deux institutions ont jusqu'ici notifié toutes leurs opérations de traitement existantes au CEPD pour contrôle préalable. Toutefois, la plupart des institutions ont indiqué que toutes les opérations de traitement déterminées seraient notifiées au CEPD d'ici à la fin de 2009.

Principaux résultats dans les agences

Le CEPD a constaté que des **progrès positifs** avaient été effectués dans la détermination des opérations de traitement et dans l'adoption de règles d'application concernant les missions et les fonctions du DPD. Toutefois, le taux de notification des opérations de traitement au DPD et de notification au CEPD pour contrôle préalable était généralement très faible. Seule une agence a affirmé que toutes les opérations déterminées avaient été notifiées au CEPD.

Même si les demandes d'accès aux données au titre du règlement ont été peu nombreuses, voire inexistantes, le CEPD a constaté avec plaisir que les agences envisageaient de mettre sur pied des outils de contrôle pour suivre ces demandes.

Étapes ultérieures

Le CEPD encouragera et suivra de près les évolutions futures, en particulier dans les institutions et agences qui devaient améliorer leur respect du règlement dans le domaine du contrôle préalable par le CEPD et des notifications au DPD. Des enquêtes complémentaires concernant le respect du règlement suivront pour évaluer les progrès futurs.

2.5.2. Enquêtes

Les enquêtes constituent un outil indispensable pour que le CEPD puisse surveiller et assurer l'application des dispositions du règlement et se basent sur ses articles 41, paragraphe 2, 46, point c), et 47, paragraphe 2.

Les pouvoirs étendus qui sont conférés au CEPD lui permettant d'accéder à toutes les informations et données à caractère personnel nécessaires à ses enquêtes et d'obtenir l'accès à tous les locaux dans lesquels le responsable du traitement ou une institution ou un organe de l'UE exerce ses activités ont pour objet de lui permettre de disposer de moyens efficaces pour s'acquitter de ses fonctions. Les enquêtes peuvent résulter d'une réclamation ou être effectuées de la propre initiative du CEPD.

L'article 30 du règlement prévoit que les institutions et organes de l'UE sont tenus de coopérer avec le CEPD dans l'accomplissement de ses fonctions et doivent lui communiquer les informations demandées et lui accorder l'accès requis.

Au cours des enquêtes, le CEPD **vérifie les faits sur place,** son objectif étant également d'assurer le respect du règlement. Les enquêtes sont suivies d'un retour d'informations adéquat à l'institution ou à l'organe qui fait l'objet de l'enquête.

En 2009, le CEPD a poursuivi les enquêtes annoncées dans le cadre de l'exercice «printemps 2007», notamment au Parlement européen et à l'EPSO, et a démarré une enquête à la Cour des comptes européenne. En juillet 2009, sur la base de l'expérience acquise au cours des enquêtes, le CEPD a adopté un manuel interne de procédure d'enquête et a publié les éléments clés de cette procédure sur son site internet.

Politique et procédures d'enquête du CEPD

Le **manuel interne relatif aux enquêtes** du CEPD vise à fournir des orientations au personnel du CEPD. Il se base essentiellement sur le cadre

juridique existant, sur les principes généraux du droit européen et sur les bonnes pratiques administratives communes aux institutions et organes de l'UE.

Le manuel contient des détails sur la procédure administrative, les fonctions des inspecteurs et la politique de sécurité, ainsi que des formulaires types pour la production de documents d'enquête. Il explique les finalités de ces documents et donne des conseils utiles pour la préparation d'une enquête.

Le manuel d'enquête est un document vivant, soumis à une révision régulière à mesure que les pratiques et les expériences du CEPD évoluent. Un document thématique sur le rôle des enquêtes et sur les critères de réalisation d'une enquête sera élaboré en temps voulu.

Enquête au Parlement européen

En février 2009, le CEPD a mené une enquête au Parlement européen. Cette enquête portait sur des faits relatifs à des opérations de traitement des données à caractère personnel par les services médicaux à Bruxelles et à Luxembourg et par le service des absences médicales, en relation avec les trois avis relatifs au contrôle préalable émis par le CEPD. Elle visait également à vérifier la mise en œuvre des recommandations émises dans ces avis. L'obligation pour les responsables du traitement des données à la direction générale des politiques externes (DG EXPO) de notifier au DPD les opérations de traitement des données à caractère personnel en vertu de l'article 25 du règlement constituait également une partie de l'enquête.

À l'issue de l'enquête, le CEPD a exprimé des inquiétudes concernant certaines déficiences dans le domaine de la **sécurité de l'information dans les services médicaux** (organisationnelles, physiques et techniques), suggérant que des améliorations substantielles étaient nécessaires. En particulier, le CEPD a appelé à trouver une solution adéquate au transfert des rapports médicaux du service des absences médicales au service médical.

Le CEPD a envoyé une liste de recommandations au secrétaire général du Parlement lui demandant de prendre les mesures appropriées. Plusieurs de ces mesures ont ensuite été mises en œuvre, mais le suivi de cette enquête se poursuit.

Enquête à l'Office européen de sélection du personnel

En mars 2009, le CEPD a effectué une enquête à l'Office européen de sélection du personnel. L'enquête portait sur les opérations de traitement de données à caractère personnel en relation avec plusieurs contrôles préalables effectués dans le domaine de la sélection des fonctionnaires, agents temporaires et agents contractuels, ainsi que toute opération connexe de traitement des données à caractère personnel.

L'enquête a montré que l'EPSO avait accompli des **progrès considérables en matière de transparence** de ses procédures et des informations fournies aux candidats. Dans ses conclusions, le CEPD a toutefois rappelé l'obligation pour l'EPSO de fournir aux candidats qui le souhaitent des fiches d'évaluation établies par le jury lors des examens oraux. L'accès aux questions des tests à choix multiples n'a pas été établi au cours de l'enquête car il fait actuellement l'objet d'une procédure judiciaire.

En ce qui concerne la **politique de conservation,** le CEPD a exprimé le souhait qu'une procédure documentée soit mise en œuvre pour l'archivage des dossiers dans les archives historiques de la Commission.

L'enquête visait également à vérifier la conformité de **certaines bases de données et de certains outils informatiques de l'EPSO** utilisés dans les procédures de sélection. Le CEPD a pris une mesure générale demandant que les mesures techniques et organisationnelles de sécurité soient documentées et plus systématiquement intégrées dans les procédures de concours.

Les conclusions de l'enquête ont été envoyées au directeur de l'EPSO, qui a adopté un plan d'action sur la base des recommandations émises par le CEPD. Étant donné que ce plan d'action fait partie d'un plan d'amélioration continue et que les procédures sont revues en conséquence, le CEPD a suspendu ses conclusions finales jusqu'au début de 2010.

Enquête à la Cour des comptes européenne

En mars 2009, le CEPD a procédé à une enquête à la Cour des comptes (CdC) en relation avec le contrôle du personnel (contrôle de l'internet et rapport sur l'outil d'audit).

Le CEPD a salué l'utilisation par la CdC de **techniques de filtrage** qui facilitent l'approche préventive de l'abus de l'internet plutôt que l'utilisation de l'approche répressive. Il est à noter que le CEPD a rejeté les caractéristiques et les fonctions des filtres logiciels utilisés pour contrôler les tentatives avortées d'accéder à l'internet et a souligné l'importance des **études d'impact sur la vie privée** en tant qu'outils à utiliser dans le processus de sélection des logiciels à des fins de surveillance. Le CEPD a également estimé qu'il convenait d'étendre les principes de ***Privacy by Design*** (respect de la vie privée dès la conception) à l'ensemble du processus de conception de l'internet et des systèmes et processus de contrôle des réseaux. Le CEPD a invité la CdC à améliorer les politiques visant à maintenir un **niveau de conformité en matière de sécurité élevé** de manière à mettre sur pied une procédure de surveillance de l'internet solide, sûre, équitable et respectueuse de la vie privée et des règles applicables en matière de protection des données.

En ce qui concerne l'aspect de l'enquête relatif à la consultation concernant une procédure d'**accès au disque/courrier électronique privé des membres du personnel,** le CEPD a analysé les objectifs pertinents et les pratiques actuelles à la CdC et conclu qu'il existait un risque de violation de la confidentialité des communications. En conséquence, le CEPD a souligné qu'une notification formelle en vue d'un contrôle préalable devait lui être soumise concernant ce traitement, qui présente un risque spécifique au titre de l'article 27, paragraphe 1, du règlement.

L'enquête s-TESTA

Le réseau s-TESTA (services télématiques transeuropéens sécurisés entre administrations) fournit une infrastructure générale pour répondre aux besoins en matière de gestion des opérations et d'échanges d'informations entre les administrations européennes et nationales. Actuellement, plus de 30 applications se basent sur ce réseau sécurisé fourni par la Commission européenne.

Le CEPD, en sa qualité d'autorité de supervision des systèmes et des applications informatiques de la Commission qui traitent des données à caractère personnel, a décidé de procéder à une enquête du réseau s-TESTA, et plus particulièrement de son centre de service et d'opération (CSO) situé à Bratislava en septembre 2009. La Commission européenne a confié la gestion du CSO à un sous-traitant, Orange Business Service/Hewlett Packard (OBS/HP). L'objectif principal de l'enquête était de collecter des éléments sur les mesures mises en œuvre dans le domaine de la sécurité et de la protection des données et de comparer celles-ci aux exigences définies dans le contrat et aux réglementations correspondantes. Dans ce cadre, l'enquête du CEPD a été axée sur les infrastructures du CSO ainsi que sur son personnel, son organisation et ses technologies.

Le CEPD a été globalement satisfait des mesures de sécurité demandées par la Commission et mises en œuvre par OBS/HP sur les systèmes, applications et processus organisationnels informatiques du CSO. Le lancement de différentes mises à jour de sécurité et la mise en œuvre d'un plan d'amélioration continue fourniront un mécanisme de protection des données encore plus fort.

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 des 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 (par exemple modalités d'application du règlement, règles internes ou 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 sur des dossiers particuliers supposant des traitements ou sur des questions abstraites relatives à l'interprétation du règlement.

Dans le cadre des consultations menées sur des mesures administratives envisagées par une institution ou un organe, plusieurs questions ont été évoquées, notamment:

- les transferts de données à caractère personnel aux pays tiers;
- le traitement des données à caractère personnel dans le cadre d'une procédure en cas de pandémie;
- l'exercice du droit d'accès;
- l'application des règles en matière de protection des données au service d'audit interne;
- les modalités d'application du règlement (CE) n° 45/2001.

2.6.1. Transferts de données à caractère personnel aux pays tiers

L'**Office européen de lutte antifraude** a soulevé la question de savoir si trois groupes de pays pouvaient être considérés comme présentant un **niveau de protection des données adéquat,** à la lumière de leur relation avec la convention 108 du Conseil de l'Europe et son protocole additionnel.

L'OLAF a également demandé — si l'on estimait qu'un ou plusieurs de ces groupes ne présentaient pas un niveau adéquat de protection au sens du règlement sur la protection des données (article 9, paragraphe 1) — si les engagements pris dans le contexte de la convention et/ou des accords d'assistance administrative mutuelle dans le domaine douanier seront considérés comme des «garanties suffisantes» (article 9, paragraphe 7) (dossier 2009-0333).

À l'issue de l'analyse, le CEPD a conclu qu'il n'y avait **pas suffisamment de preuves** de la mise en œuvre satisfaisante de la convention 108 et de son protocole additionnel dans les pays concernés. En conséquence, en principe, on ne pouvait considérer que les trois groupes de pays présentaient un niveau de protection adéquat.

Le CEPD a ajouté que l'OLAF pouvait néanmoins effectuer une évaluation de la possibilité ou de l'impossibilité de procéder à un transfert particulier (ou un ensemble de transferts), limité à des objectifs spécifiques et à certains destinataires dans le pays de destination, qui présentent effectivement un niveau de protection adéquat. Une telle évaluation impliquerait un examen de la législation nationale qui met en œuvre la convention et son protocole, ainsi que leur mise en œuvre effective.

Le CEPD a également mentionné qu'une troisième possibilité serait que l'OLAF et les destinataires introduisent des garanties adéquates.

2.6.2. Traitement des données à caractère personnel dans le cadre d'une procédure en cas de pandémie

Le CEPD a été consulté sur la question du traitement de données à caractère personnel dans le cadre de la procédure en cas de **pandémie** élaborée par la **Banque centrale européenne** (dossier 2009-0456). Hormis les traitements des données à caractère personnel par les services médicaux de la BCE, en cas de pandémie, il faudrait également informer l'encadrement local qu'une personne donnée est suspectée d'avoir été contaminée afin que les membres concernés de l'équipe puissent être alertés.

Le CEPD a estimé qu'en l'absence d'une quelconque obligation légale nationale, l'article 5, point a), du règlement pouvait servir de base juridique pour le traitement des données dans le cadre de la procédure en cas de pandémie, mais que, étant donné le caractère exceptionnel de cette procédure, il serait souhaitable qu'une décision formelle soit prise par la BCE sur laquelle toute communication aux services d'encadrement pourrait être fondée.

Le CEPD a ensuite souligné que comme le traitement portait sur des données relatives à la santé, il était interdit, sauf exceptions prévues à l'article 10 du règlement. Le traitement des données relatives à la santé pourrait donc se baser sur une obligation juridique pour les employeurs de respecter les obligations en matière de santé et de sécurité au travail. Le CEPD a également estimé que dans le cas présent, des raisons d'«intérêt public crucial» pouvaient justifier le traitement des données relatives à la santé, mais que des garanties adéquates devaient être mises en place pour protéger les intérêts des personnes concernées.

2.6.3. L'exercice du droit d'accès

Le CEPD a été consulté par l'**OLAF** sur un dossier hypothétique lié principalement à l'exercice du **droit d'accès** (dossier 2009-0550).

Le CEPD a estimé que la demande d'une liste des dossiers dans lesquels apparaissent les données à caractère personnel de la personne concernée

doit en principe être couverte par l'article 13, point a), du règlement étant donné qu'il s'agit d'une manière d'obtenir «la confirmation que des données la concernant sont ou ne sont pas traitées». La manière dont la «confirmation» sera fournie dépend, dans une certaine mesure, de la nature et des caractéristiques des données et de l'activité de traitement concernée. Elle dépend également du fait ou non qu'un mode particulier de fourniture des données permette à la personne concernée d'exercer ses différents droits de protection des données ([7]).

Une approche au cas par cas doit être suivie dans l'évaluation des méthodes et paramètres d'accès. Les informations fournies à la personne concernée doivent être «compréhensibles» («intelligibles») et stipuler quelle activité de traitement a lieu et quelles données sont concernées. Le niveau de détail devrait permettre à la personne concernée d'évaluer l'exactitude des données et la licéité du traitement, ainsi que refléter la charge de travail pour le responsable du traitement.

2.6.4. Application des règles de protection des données au service d'audit interne

En prévision d'un audit à venir sur la gestion des ressources humaines à l'Agence européenne des médicaments, le chef de l'administration de l'EMA a demandé au CEPD de confirmer si le règlement était applicable à l'équipe du service d'audit interne (SAI) au cours de l'audit (dossier 2009-0097).

Le CEPD a estimé que le SAI était un organe communautaire qui traitait des données personnelles dans le cadre de ses activités et qu'il relevait du droit communautaire, applicable à ce stade. Ainsi, si le SAI devait avoir accès à des données à caractère personnel au cours de ses activités d'audit, cet accès serait régi par les dispositions du règlement.

2.6.5. Dispositions d'application du règlement (CE) n° 45/2001

Plusieurs DPD ont consulté le CEPD sur des projets de dispositions d'application du règlement (CE) n° 45/2001 établis par leur agence. Le CEPD a relevé que tous les projets portaient non seulement sur les tâches, fonctions, et compétences des DPD (article 24, paragraphe 8, et annexe du règlement), mais aussi sur le rôle des responsables du traitement et les droits des personnes concernées. Certaines recommandations du CEPD revêtant une importance particulière portaient sur les questions suivantes:

- le DPD devrait s'assurer de l'application interne des dispositions du règlement **de manière indépendante,** sans recevoir d'instructions de qui que ce soit (dossiers 2009-0656 et 2009-0684);
- le DPD peut avoir recours à une **assistance extérieure,** pour autant qu'elle ne remette pas en cause son indépendance (dossier 2009-0656);
- si nécessaire, une **formation à la protection des données** devrait être organisée par l'agence (dossier 2009-0656);
- le personnel d'appui du DPD devrait être soumis à la même obligation de **secret professionnel** que le DPD (dossier 2009-0684);
- le **comité du personnel** devrait également pouvoir consulter le DPD, et en général, celui-ci peut être consulté sans passer par les canaux officiels (dossiers 2009-0684, 2009-0204 et 2009-0163).

2.7. Lignes directrices thématiques

L'expérience acquise grâce à l'application du règlement (CE) n° 45/2001 a permis au personnel du CEPD de traduire leur expertise en une orientation générale pour les institutions et organes. En 2009, le CEPD a élaboré des lignes directrices sur des thèmes spécifiques sous la forme de documents thématiques.

2.7.1. Lignes directrices en matière de recrutement

Les orientations du CEPD concernant les opérations de traitement des données en matière de recrutement de personnel (adoptées à la fin de 2008) examinent le cycle des procédures administratives

([7]) Voir point 57 de l'arrêt de la Cour de justice dans l'affaire C-553/07, *Rotterdam contre Rijkeboer.*

Lorsqu'elles recrutent du personnel, les institutions de l'UE doivent veiller à ne collecter que des données pertinentes.

(sélection, recrutement et modalités contractuelles) mises en œuvre pour recruter du personnel permanent, contractuel et temporaire, ainsi que des experts nationaux et des stagiaires.

Entre autres choses, les orientations analysent **la collecte** par les institutions de données relatives aux **condamnations antérieures** afin de respecter le statut des fonctionnaires: une personne ne peut être recrutée que si elle jouit pleinement de ses droits civiques et qu'elle offre les garanties de moralité requises pour l'exercice de ses fonctions. Le CEPD a estimé que la collecte de données concernant les condamnations pénales était licite. Il a toutefois souligné que la manière de procéder — au moyen de différents documents tels que le casier judiciaire, le fichier de police ou le certificat de bonne vie et mœurs — pouvait provoquer une collecte excessive de données. En effet, ces documents peuvent contenir des informations qui vont au-delà de l'objectif légitime consistant à vérifier que la personne jouit pleinement de ses droits.

Les orientations recommandent donc que l'analyse du contenu de ces documents soit effectuée au cas par cas, de manière à ce que seules les données pertinentes soient traitées à la lumière des exigences du statut des fonctionnaires.

En ce qui concerne le **délai de conservation** des données relatives aux condamnations pénales, les orientations insistent sur la restitution immédiate de l'extrait de casier judiciaire à la personne après la sélection et le recrutement éventuel. Ces documents sont des instantanés qui ne sont peut-être déjà plus exacts le lendemain de leur production. Un formulaire standard indiquant que la personne est apte à exercer ses fonctions et qu'elle jouit pleinement de ses droits civiques pourrait donc être créé à des fins de preuves et de contrôle.

Les orientations analysent également les **transferts externes** de données soit aux entreprises qui organisent des tests au nom du comité de sélection, soit aux experts externes nationaux recrutés en tant que membres du comité de sélection. La nécessité de ces transferts devrait être établie conformément à l'article 8, point a). En outre, le mandat précis des sous-traitants extérieurs doit être défini dans un contrat ou un acte juridique. Leurs obligations doivent également être établies conformément aux obligations de confidentialité et de sécurité visées à l'article 23 du règlement.

2.7.2. Lignes directrices sur les données en matière de santé

En septembre 2009, le CEPD a publié des lignes directrices sur le traitement des données en matière de santé sur le lieu de travail par les institutions et organes de l'UE.

Les lignes directrices examinent la **base juridique** du traitement des données en matière de santé par les institutions et organes de l'UE, tel qu'établi principalement par le statut des fonctionnaires, et

déterminent pour quelles finalités et dans quelles conditions les données en matière de santé peuvent être traitées. Par exemple, le statut des fonctionnaires prévoit le traitement des données en matière de santé en relation avec un examen médical de prérecrutement afin de déterminer si le futur membre du personnel est apte physiquement à exercer ses fonctions. Le statut des fonctionnaires ne prévoit toutefois pas que le même examen médical de prérecrutement serve également des objectifs de prévention. Cela étant dit, le CEPD reconnaît que les données collectées au cours de cet examen médical pourraient en plus servir à alerter un futur membre du personnel au sujet d'un problème de santé spécifique et pourraient donc servir des objectifs de prévention. Cela ne veut toutefois pas dire que des informations supplémentaires devraient être demandées à des fins de prévention.

Les lignes directrices appliquent également **le principe de qualité des données.** Ce principe implique une évaluation de tous les questionnaires médicaux soumis aux membres du personnel afin de veiller à ce que seules les données nécessaires et pertinentes soient collectées et traitées. Si la personne concernée se voit proposer de faire un test du virus d'immunodéficience humaine (VIH) au cours de la visite médicale, il faut préciser clairement que ce test n'est pas obligatoire et qu'il ne peut se faire qu'avec le consentement spécifique et informé de la personne concernée. Le principe de la qualité des données pousse également le CEPD à conclure que si un membre du personnel décide de passer son examen médical annuel chez le médecin de son choix, les résultats de cette visite ne doivent être communiqués aux services médicaux des institutions qu'avec le consentement libre et informé de la personne concernée.

2.7.3. Lignes directrices en matière de vidéosurveillance

Le 7 juillet 2009, le CEPD a publié une version de consultation des lignes directrices en matière de vidéosurveillance. Tous les intéressés étaient invités à fournir un retour d'information par écrit et un atelier a été organisé à Bruxelles le 30 septembre 2009. Près d'une centaine de délégués à la protection des données, de responsables de la sécurité, de spécialistes en vidéosurveillance et en technologies de l'information ainsi que des représentants du personnel de plus de quarante institutions et organes de l'UE étaient présents.

L'atelier et le processus de consultation ont atteint leur double objectif d'obtenir un retour d'informations pour améliorer les projets de lignes directrices et de renforcer la coopération pour veiller au respect des principes de protection des données.

Giovanni Buttarelli, contrôleur adjoint, s'exprimant lors de l'atelier du CEPD dédié aux projets de lignes directrices sur la vidéosurveillance (Bruxelles, le 30 septembre 2009).

Globalement, les réactions aux projets de lignes directrices ont été positives. Dans un climat d'inquiétude croissante quant à l'augmentation de l'utilisation de la surveillance, les participants ont salué le fait que les projets de lignes directrices fournissent des conseils pratiques leur permettant de décider s'il faut utiliser les équipements de vidéosurveillance et de trouver le meilleur moyen de traiter des questions de protection des données.

Objectifs des lignes directrices en matière de vidéosurveillance et principes essentiels

Le CEPD souhaitait publier ces lignes directrices au début de 2010, dans le double objectif i) de contribuer à réduire et à empêcher la prolifération incontrôlée de la vidéosurveillance lorsqu'elle n'est pas justifiée et ii) d'aider les institutions à utiliser la vidéosurveillance de manière responsable et à instaurer des garanties lorsque l'utilisation de la vidéosurveillance est justifiée.

Thèmes clés abordés dans les lignes directrices

- *Comment sélectionner, installer et configurer un système?*
- *Combien de temps les enregistrements doivent-ils être conservés?*
- *Qui a accès aux images?*
- *Quelles mesures de sécurité faut-il prendre pour protéger les données?*
- *Comment informer le public?*
- *Comment répondre aux demandes d'accès?*

Les lignes directrices sont conçues pour encourager la prise de décision au niveau local, sur la base des besoins de sécurité locaux, tout en tenant compte des préoccupations spécifiques des autres parties prenantes, notamment du personnel. Elles soulignent également la responsabilité des institutions et recommandent d'adopter une politique officielle en matière de vidéosurveillance et de procéder à des contrôles périodiques pour garantir et démontrer le respect des règles. Enfin, elles encouragent les institutions à intégrer la protection de la vie privée et des données dans la technologie qu'elles développent, ainsi que dans leurs pratiques organisationnelles, dans le respect du principe *Privacy by Design*.

Nécessité et proportionnalité

Les lignes directrices sont fondées sur les principes de nécessité et de proportionnalité, ce qui devrait réduire les données au minimum et aider à mettre fin à la prolifération incontrôlée des caméras de sécurité. Les décisions quant à l'installation de caméras et la manière de les utiliser ne doivent pas être prises en se basant uniquement sur les besoins de sécurité. Au lieu de cela, ces besoins doivent être mis en balance avec le respect des droits de fondamentaux de l'individu.

Questions à poser avant d'installer un système

- *Quels sont les bénéfices de l'utilisation de la vidéosurveillance?*
- *L'objectif du système est-il clairement spécifié, explicite et légitime?*
- *La vidéosurveillance se base-t-elle sur un fondement licite?*
- *La nécessité de la vidéosurveillance est-elle clairement démontrée?*
- *Est-ce la meilleure manière d'atteindre les objectifs fixés?*
- *Existe-t-il d'autres solutions moins intrusives?*
- *Les bénéfices sont-ils supérieurs aux effets négatifs?*

Cela étant dit, la protection des données ne doit pas empêcher les services répressifs de faire leur travail. Les besoins de sécurité et la protection des données sont souvent décrits comme des notions opposées, difficiles à réconcilier. Toutefois, les droits fondamentaux et la sécurité ne doivent pas s'exclure mutuellement. Grâce à une approche pragmatique basée sur le double principe de la sélectivité et de la proportionnalité, les systèmes de surveillance peuvent répondre aux besoins de sécurité tout en respectant la vie privée. Il convient d'utiliser la technologie de surveillance de manière ciblée, en réduisant au minimum la collecte de données non pertinentes. Non seulement cela réduira les intrusions dans la vie privée, mais cela contribuera à garantir une utilisation de la surveillance plus ciblée, et en fin de compte plus efficace, pour répondre au problème de la sécurité. Pour conclure, le CEPD estime qu'il est nécessaire d'adopter une approche sélective de l'utilisation des systèmes de surveillance, afin que le public ne fasse pas l'objet de restrictions excessives à la suite d'actions d'une minorité.

La vidéosurveillance doit être utilisée de manière responsable et assortie de garanties efficaces.

Privacy by Design et responsabilité

La protection de la vie privée et des données ne peut être garantie uniquement en «cochant» des cases de conformité. Lorsque c'est possible, une approche préventive doit être utilisée: la vie privée doit être «intégrée dès la conception» dans les systèmes de technologies de l'information et de la communication (TIC) et les pratiques organisationnelles. Non seulement la notion de *Privacy by Design* porte sur la conception et les solutions techniques des systèmes TIC, mais elle requiert également des pratiques responsables et respectueuses de la vie privée ainsi que des infrastructures physiques respectueuses de la vie privée. La vidéosurveillance est un domaine où les principes de *Privacy by Design* peuvent se révéler particulièrement utiles et pertinents.

Les systèmes de vidéosurveillance conçus à des fins de sécurité ou pour d'autres types de surveillance devraient toujours être élaborés selon le principe de *Privacy by Design* et les exigences en matière de protection des données devraient faire partie intégrante du développement de ces systèmes. Les systèmes de traitement des données devraient être conçus et sélectionnés en vue de réduire au minimum la collecte et l'utilisation des données à caractère personnel. Les concepteurs des systèmes devraient également déterminer et faire le meilleur usage des techniques disponibles. Les préoccupations en matière de protection des données doivent également être prises en considération de manière précoce. Les raisons sont évidentes: une fois qu'un système est en place, il est plus difficile d'inclure des solutions respectueuses de la protection des données, par exemple pour garantir les niveaux nécessaires de sécurité, donner différents niveaux d'accès et garantir un suivi fiable de l'enregistrement des données et les droits d'accès des personnes concernées.

La responsabilisation *(accountability)* signifie qu'une organisation responsable (le responsable du traitement) doit être capable de démontrer qu'elle respecte ses obligations en matière de protection des données. Elle encourage l'utilisation des évaluations de l'impact et des audits relatifs à la protection des données et à la vie privée et déplace l'équilibre du respect de la vie privée des contrôles par les autorités réglementaires vers des mesures proactives prises par les responsables eux-mêmes. La nécessité de démontrer le respect des règles aux parties prenantes et aux autorités réglementaires signifie également que la responsabilisation entraîne une transparence accrue, par exemple, en rendant publique la politique de vidéosurveillance d'une organisation.

Systèmes standard contre contrôle accru

Les lignes directrices sont conçues pour fournir des garanties de protection des données détaillées pour la plupart des systèmes standards de vidéosurveillance gérés à des fins de sécurité commune. Ainsi, dans la majorité des cas, il n'est pas nécessaire de procéder à une étude plus formelle et approfondie de l'impact sur la protection des données d'un système de vidéosurveillance par une institution, d'introduire de nouvelles garanties ou

de soumettre des plans de surveillance au CEPD pour contrôle préalable. Il suffit de suivre les lignes directrices et de les appliquer.

Toutefois, si la surveillance proposée augmente significativement les risques pour les droits fondamentaux et les intérêts légitimes des personnes sous surveillance (par rapport aux systèmes standards de vidéosurveillance et aux garanties décrites dans les lignes directrices), une étude d'impact sur la protection de la vie privée et des données doit être effectuée avant d'installer et de mettre en œuvre le système. L'objectif de cette étude est de déterminer les incidences supplémentaires du système proposé sur la vie privée et les autres droits fondamentaux d'un individu et de déterminer les moyens de réduire ou d'éviter les conséquences négatives. Ces systèmes sont soumis au contrôle préalable et seront suivis de près par le CEPD.

Suivi approfondi
- *Surveillance des employés et des bureaux individuels*
- *Surveillance dissimulée et utilisation de la vidéosurveillance dans les enquêtes*
- *Surveillance des manifestants*
- *Vidéosurveillance haute technologie ou intelligente (par exemple reconnaissance des visages, surveillance dynamique préventive)*
- *Systèmes interconnectés*
- *Enregistrements sonores et «CCTV parlante»*

2.8. Eurodac

Eurodac a été créé par le règlement (CE) n° 2725/2000 du Conseil («règlement Eurodac») qui, avec le règlement Dublin II, est en cours de révision. 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'Union européenne. Ce système contribue à l'application effective du règlement Dublin II, qui détermine l'État membre de l'UE responsable de l'examen des demandes d'asile des personnes qui demandent la protection internationale au titre de la convention de Genève au sein de l'Union européenne.

Le CEPD est chargé de **contrôler le traitement des données à caractère personnel contenues dans la base de données centrale du système géré par la Commission et leur transmission** aux États membres. À ce titre, il coopère étroitement avec les autorités nationales de protection des données dans les États membres qui contrôlent le traitement des données au niveau national ainsi que la transmission des données à l'unité centrale. Les représentants des autorités chargées de la protection des données et le CEPD se réunissent régulièrement pour examiner des problèmes communs liés au fonctionnement du système.

Ce **«modèle de supervision coordonnée»** est un très bon exemple d'approche coordonnée de supervision de la protection des données (voir section 4.3).

Les activités du CEPD relatives à Eurodac comprennent notamment des consultations et des conseils, dans le cadre de la révision des règlements Eurodac et Dublin en cours de discussion au sein des institutions de l'UE. En février 2009, le CEPD a émis deux avis en la matière (voir la section 3.3.2).

3

CONSULTATION

3.1. Introduction: aperçu et tendances

Plusieurs activités et événements importants qui ont eu lieu en 2009 ont contribué à nous rapprocher de l'**objectif d'un nouveau cadre juridique de protection des données.** La réalisation de cet objectif sera un volet important de l'agenda du CEPD pour les prochaines années.

À la fin de 2008, un cadre général de protection des données dans le domaine de la coopération policière et judiciaire a été adopté pour la première fois au niveau européen (décision-cadre 2008/977/JAI du Conseil). En 2009, un deuxième développement législatif majeur a eu lieu.

La première mise à jour du cadre juridique de la protection des données — la directive 2002/58/CE «Vie privée et communications électroniques» — a été révisée par la directive 2009/136/CE du 25 novembre 2009.

Toutefois, ce n'est que le début.

L'entrée en vigueur du traité de Lisbonne marque le début d'une nouvelle ère pour la protection des données. L'article 16 TFUE contient non seulement un droit individuel pour la personne concernée, mais enjoint également au Parlement européen et au Conseil d'assurer la protection des données dans tous les domaines du droit de l'UE.

En d'autres termes, elle permet l'application d'un cadre juridique global de protection des données au secteur privé, au secteur public dans les États membres et aux institutions et organes de l'UE.

Le programme de Stockholm — Une Europe ouverte et sûre au service des citoyens, approuvé par le Conseil européen de décembre 2009, souligne que l'Union doit prévoir une stratégie globale de protection des données au sein de l'UE et dans ses relations avec les autres pays. Dans son avis sur le programme de Stockholm, le CEPD souligne la nécessité d'un nouveau cadre législatif, remplaçant entre autres la décision-cadre 2008/977/JAI du Conseil.

L'étape la plus importante dans ce contexte est toutefois la consultation publique sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, organisée par la DG Justice, liberté et sécurité.

Cette consultation publique doit être considérée comme un premier pas sur la voie d'un instrument juridique moderne et global de protection des données reflétant pleinement les changements apportés par le traité de Lisbonne, et elle garantira la protection effective des données à caractère personnel dans la société de l'information.

La contribution conjointe du groupe de l'article 29 et du groupe de travail sur la police et la justice intitulée «L'avenir de la protection de la vie privée» a été adoptée en décembre 2009 avec le soutien total et des contributions importantes du CEPD. Ce

document devrait bénéficier d'une forte attention car il constitue l'avis pertinent de la communauté européenne de la protection des données concernant le développement du cadre juridique moderne et global mentionné plus haut.

Dans le contexte global, il est important de noter que la 31e conférence internationale des autorités de protection des données et de la vie privée, qui s'est tenue à Madrid en novembre 2009, a adopté une résolution sur les normes internationales en matière de protection des données. En ce qui concerne la protection des données au niveau transatlantique, des étapes ont été franchies en vue d'arriver à un accord entre l'UE et les États-Unis sur l'échange de données à caractère personnel à des fins répressives.

L'année 2009 peut également être caractérisée comme une année où le CEPD a abordé deux autres domaines de la politique européenne dans lesquels le traitement des données à caractère personnel revêt une importance essentielle: les listes de terroristes et la fiscalité.

La politique relative aux «listes de terroristes» s'inscrit dans le cadre de la politique étrangère et de sécurité commune de l'UE. La fiscalité est quant à elle un domaine qui, par nature, implique un traitement intensif des données à caractère personnel et une coopération administrative, notamment pour lutter contre la fraude. L'accent s'est intensifié sur deux autres domaines: la santé publique et les transports. Enfin, il va sans dire que le CEPD a continué à suivre de près différentes activités de la DG Société de l'information et de la DG Justice, liberté et sécurité.

3.2. Cadre d'action et priorités

3.2.1. Mise en œuvre de la politique de consultation

Même si les méthodes de travail du CEPD dans le domaine de la consultation ont évolué au fil des ans, l'approche fondamentale des interventions n'a pas changé. Le document stratégique intitulé «Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes» ([8]) reste d'actualité, bien qu'il faille désormais le lire à la lumière du traité de Lisbonne.

([8]) Disponible sur le site internet du CEPD, à la section «Consultation».

Les avis formels du CEPD — fondés sur l'article 28, paragraphe 2, ou l'article 41 du règlement (CE) n° 45/2001 — sont les principaux instruments et contiennent une analyse complète de tous les éléments relatifs à la protection des données qui figurent dans une proposition de la Commission ou un autre instrument pertinent.

Parfois, des commentaires sont rédigés à des fins plus limitées, afin de faire passer un message rapide et fondamental ou de se concentrer sur un ou plusieurs aspects techniques.

Le CEPD est disponible à tous les stades du processus législatif et utilise toute une série d'autres instruments d'influence. Même si cela peut nécessiter des contacts étroits avec les institutions de l'UE, il est essentiel qu'il conserve son indépendance et respecte la position de toutes les autres institutions concernées.

Les contacts avec la Commission ont lieu à différents stades de la préparation des propositions, et leur intensité dépend du sujet et de l'approche des services de la Commission. Par exemple, pour les projets à long terme, comme l'e-Justice ou les discussions sur un cadre de notification des violations de la sécurité, le CEPD a contribué à différents moments et de différentes manières.

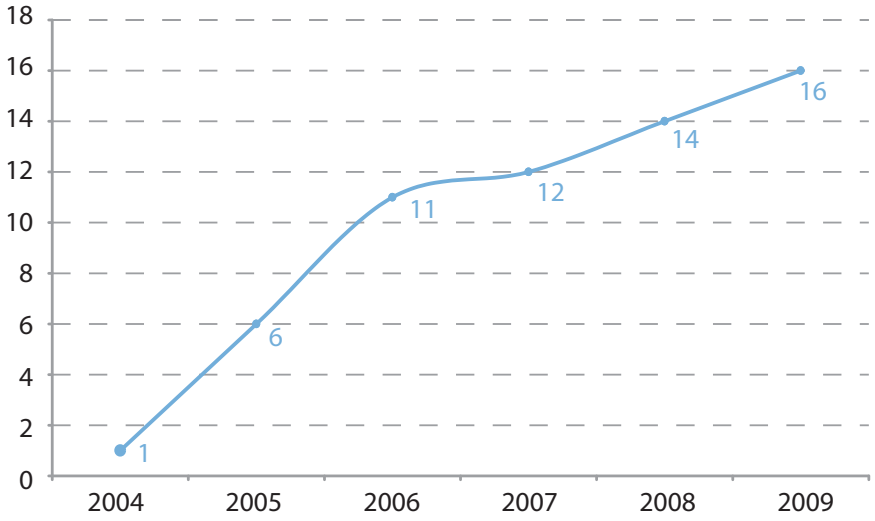
De même, des contacts ont eu lieu lors de la phase de suivi, surtout au cours des discussions et négociations intensives au Parlement ou au Conseil, conduisant à des amendements fondamentaux à une proposition de la Commission. On retrouve notamment des exemples d'implication intensive et à plusieurs stades du CEPD en 2009 dans la révision de la directive «Vie privée et communications électroniques» et la modification du règlement sur l'accès du public.

Comme mentionné plus haut, en 2009, la possibilité d'un nouveau cadre de protection des données s'est faite plus concrète, et le sujet a été abordé à plusieurs niveaux et dans plusieurs réseaux. Le CEPD a délivré son message de plusieurs manières. Il faut souligner l'importance de l'avis sur le programme de Stockholm et le rapport du groupe de l'article 29, sans négliger d'autres avis — comme celui sur l'accès des services répressifs à Eurodac — ni les discours, contributions aux conférences et discussions au Parlement européen, etc. Un des messages essentiels — à savoir qu'un cadre global est nécessaire, notamment en matière de coopération policière et judiciaire — a également été présenté par la commissaire Reding comme l'un de ses principaux objectifs.

3.2.2. Résultats en 2009

En 2009, l'augmentation rapide du nombre d'avis consultatifs s'est poursuivie. Le CEPD a émis 16 avis sur un large éventail de sujets.

Évolution des avis législatifs 2004-2009

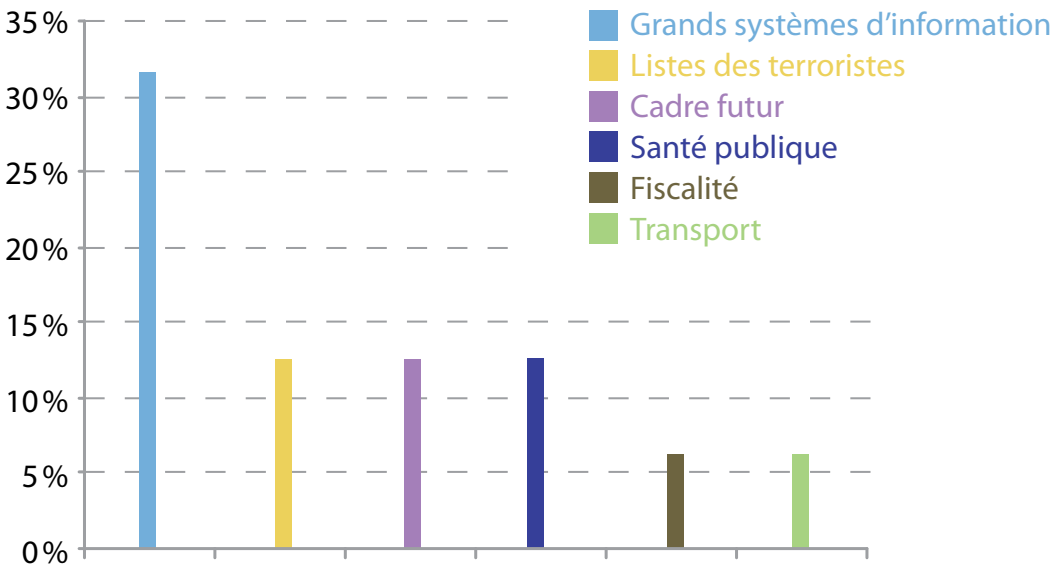


Grâce à ces avis et aux autres instruments utilisés, le CEPD a mis en œuvre les priorités pour 2009, telles que définies dans l'inventaire publié en décembre 2008. Les 16 avis couvraient différents domaines de la politique de l'UE.

L'inventaire pour 2009 a défini trois principaux domaines d'attention, à savoir la santé, la liberté, sécurité et justice, et la société de l'information. La santé publique est un domaine relativement nouveau pour le CEPD: des positions générales ont été développées dans les avis sur le don d'organes et la pharmacovigilance. Dans le domaine de la liberté, de la sécurité et de la justice, une grande attention a été accordée aux développements relatifs à la gestion des frontières et aux systèmes d'information à grande échelle. Le développement de la société de l'information figurait en bonne place de l'agenda du CEPD et le restera.

Après coup, on a constaté que, si le CEPD s'est concentré sur les priorités principales de l'inventaire 2009, les réalisations spécifiques de l'année ne correspondaient pas totalement aux intentions de l'inventaire. Cela démontre la dynamique de ce domaine. Les questions déterminées au début de l'année ne se sont pas toujours révélé les plus pertinentes au cours de l'année. Toutefois, le CEPD ne s'est pas fondamentalement départi de sa marche à suivre. Certains plans, annoncés au début de 2009, porteront leurs fruits en 2010. Cela est bien illustré par un avis émis au début de 2010 sur l'accord commercial anti-contrefaçon (ACAC).

Principaux domaines couverts par les avis législatifs en 2009



3.3. Espace de liberté, de sécurité et de justice

3.3.1. Développements généraux

Au cours de 2009, le CEPD a suivi avec un intérêt particulier les développements concernant le **programme de Stockholm,** qui présente la vision de l'UE pour les cinq prochaines années dans le domaine de la justice et des affaires intérieures. Le programme de Stockholm doit être considéré comme un pas en avant vers la construction d'un espace de liberté, de sécurité et de justice dans l'Union européenne.

Dans cet espace, la coopération entre les services répressifs, et plus généralement entre les États membres et entre les États membres et l'UE repose fortement sur la collecte et l'échange de données à caractère personnel. Il est dès lors crucial de protéger les données à caractère personnel des citoyens dans la coopération policière et judiciaire, comme le CEPD l'a souligné dans plus de 30 avis et commentaires en la matière. Le CEPD n'a cessé de souligner qu'assurer la protection des données à caractère personnel n'était pas simplement un moyen de protéger les citoyens, mais devait aussi stimuler l'application efficace de la loi et renforcer la confiance entre les services répressifs des différents États membres.

Le CEPD a émis un avis sur la communication de la Commission du 10 juin 2009 et a ensuite activement contribué — grâce à des contributions et des discours aux acteurs institutionnels concernés — au débat qui a conduit à l'adoption du programme lors du Conseil européen de décembre.

Le CEPD a soutenu l'attention accordée par le programme à la protection des droits fondamentaux, et en particulier à la protection des données à caractère personnel. De la même manière, le CEPD salue l'appel à un programme global de protection des données, qui trouve désormais une base juridique solide dans le traité de Lisbonne.

Un cadre global aiderait également à mieux traiter les tendances les plus importantes et à mieux les réglementer:

- *la **croissance exponentielle des informations numériques** avec l'évolution des technologies de l'information et de la communication;*
- *l'**internationalisation** des échanges de données à caractère personnel;*
- *l'**utilisation de données commerciales** à des fins répressives — par exemple les données collectées par des entreprises privées comme les opérateurs de télécommunications, les banques, les compagnies aériennes, etc.*

Le programme de Stockholm prévoit que l'Union mette en place une stratégie exhaustive de protection des données au sein de l'UE et dans ses relations avec les pays tiers.

Le CEPD a souligné que les institutions de l'UE devaient réfléchir aux conséquences pour les services répressifs et les citoyens européens avant d'adopter de nouveaux instruments d'échange. En outre, il a rappelé l'importance de développer et de promouvoir des normes internationales de protection des données, ainsi que de garantir que les données à caractère personnel seront transférées dans les pays tiers et les organisations uniquement lorsqu'une protection adéquate est prévue.

Le programme de Stockholm insiste sur le projet de **modèle européen d'information,** qui représente un effort salutaire visant à rationaliser et à développer une vision à long terme pour la gestion et l'échange de données à caractère personnel dans les domaines de la justice, de la sécurité, de l'asile et de l'immigration.

Le CEPD a souligné que cette perspective à long terme pouvait être utile pour établir des échanges d'informations plus efficaces tout en garantissant un niveau élevé de protection des données à caractère personnel. L'introduction de la vie privée dès la conception dans l'architecture des systèmes d'information — *Privacy by Design* ou *Privacy by Default* (vie privée par défaut) — est une étape essentielle dans la mise en œuvre de cette perspective à long terme car elle contribuera à améliorer la qualité des informations et à éviter la surcharge d'informations.

Le CEPD a également évoqué l'**interopérabilité** des différents systèmes et bases de données, qui ne devrait pas se fonder sur la technologie mais sur des choix politiques clairs et prudents. Elle doit respecter et garantir les conditions juridiques de la collecte, de l'échange et de l'utilisation des données à caractère personnel.

Les citoyens doivent être en mesure de prévoir quelles données les concernant sont collectées et dans quel but elles sont utilisées. C'est d'autant plus important lorsqu'on parle de catégories spéciales de données comme les empreintes digitales et l'ADN (acide désoxyribonucléique) ([9]).

Les nouvelles technologies seront également utilisées comme outils pour **améliorer la coopération judiciaire,** dans le cadre du projet **e-Justice** et d'autres initiatives, de manière à créer un véritable espace judiciaire européen. L'interconnexion des registres nationaux, tels que les registres d'insolvabilité, l'utilisation des vidéoconférences dans les procédures judiciaires et l'utilisation de portails internet pour améliorer l'accès des citoyens à la justice sont autant d'éléments qui s'inscrivent dans le cadre de ces initiatives, saluées par le CEPD, à condition que les principes de protection des données soient respectés lors de leur mise en œuvre. Certains de ces outils peuvent également être utilisés pour faciliter une protection plus efficace et une application plus aisée à l'échelle européenne des droits de protection des données.

([9]) Comme cela ressort également des conditions formulées par la Cour européenne des droits de l'homme dans l'affaire *S. et Marper,* 4 décembre 2008, appl. 30562/04 et 30566/04.

3.3.2. Règlements Eurodac et Dublin

Une attention particulière devrait être accordée aux questions de protection de la vie privée et des données dans le système de Dublin et Eurodac, le système à grande échelle de stockage et d'échange d'empreintes digitales des demandeurs d'asile et autres groupes d'immigrants (potentiels), qui permet de déterminer l'État membre chargé de traiter des demandes d'asile. Les personnes touchées par ce système sont parmi les **plus vulnérables de la population** et sont confrontées à de grandes difficultés en matière de défense de leurs droits.

La protection des données est également un **facteur clé du succès** pour le fonctionnement d'Eurodac, et donc pour le bon fonctionnement du système de Dublin. Des éléments tels que la sécurité des données, la qualité technique des données et la licéité de la consultation contribuent tous au bon fonctionnement du système Eurodac.

Le CEPD a adopté deux avis connexes concernant la proposition de révision du «règlement Eurodac» et la proposition de refonte du règlement de Dublin, qui détermine l'État membre de l'UE chargé de traiter une demande d'asile.

Ces propositions visent à assurer un niveau plus élevé d'harmonisation, une efficacité accrue et de meilleures normes de protection du régime d'asile européen commun. Elles sont également particulièrement pertinentes pour le CEPD, étant donné son rôle actuel en tant qu'autorité de contrôle d'Eurodac.

Dans ces avis, le CEPD a soutenu les objectifs de la révision et salué l'attention considérable accordée aux deux propositions sur le respect des droits fondamentaux des ressortissants de pays tiers et des apatrides. Le CEPD a émis plusieurs observations concernant, entre autres, le respect des droits de la personne concernée, la supervision du système et les mécanismes de partage d'information.

La Commission a également proposé d'autoriser l'accès au système Eurodac — destiné à faciliter l'application du règlement de Dublin en comparant les empreintes digitales des demandeurs d'asile et des immigrés clandestins — aux services répressifs à des fins de prévention, de détection et d'investigation des infractions terroristes, ainsi que d'autres infractions moins graves aux conditions décrites dans les propositions.

Le CEPD a analysé les propositions au regard de leur proportionnalité et leur légitimité, en prenant comme point de départ la nécessité de trouver le juste équilibre entre le besoin de sécurité publique et le droit fondamental à la protection de la vie privée et des données, conformément à l'article 8 de la convention européenne des droits de l'homme (CEDH).

L'analyse a conduit à la conclusion que la nécessité et la proportionnalité des propositions, qui sont des éléments essentiels pour justifier l'intrusion dans la vie privée, n'ont pas été démontrées.

Le CEPD a recommandé d'évaluer la légitimité des propositions dans un contexte plus large, notamment:

- la tendance à octroyer aux services répressifs un accès aux données à caractère personnel des individus qui ne sont suspectés d'aucun crime et qui ont été collectées à d'autres fins;
- la nécessité d'une évaluation au cas par cas de chaque proposition de ce type;
- la nécessité d'une vision cohérente, globale et orientée vers l'avenir, liée de préférence au programme-cadre de cinq ans pour la justice et les affaires intérieures («programme de Stockholm»).

3.3.3. Agence pour la gestion opérationnelle des systèmes d'information à grande échelle

La Commission a proposé un paquet législatif établissant une Agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice.

L'Agence serait responsable de la gestion opérationnelle du système d'information Schengen (SIS II), du système d'information sur les visas (VIS), d'Eurodac et éventuellement d'autres systèmes d'information à grande échelle.

Comme ces bases de données contiennent **un grand nombre de données à caractère personnel** (par exemple détails des passeports, visas et empreintes digitales), dont certaines sont sensibles, le CEPD a analysé la proposition afin de veiller à ce que l'**impact sur la vie privée des individus** soit suffisamment pris en considération dans l'instrument législatif.

Le CEPD estime qu'il y a des avantages à créer une Agence pour la gestion opérationnelle de certains systèmes d'information à grande échelle, mais uniquement si elle est établie dans son domaine d'activité et si ses responsabilités sont clairement définies.

La création d'une Agence pour la gestion opérationnelle de bases de données à grande échelle doit être fondée sur une législation non ambiguë pour ce qui est de ses compétences et de ses activités. Cette clarté empêchera toute mauvaise compréhension à l'avenir concernant les activités de l'Agence et évitera le risque de détournement d'usage. Les propositions, telles qu'elles sont rédigées actuellement, ne respectent pas ces exigences.

3.3.4. Système d'information douanier (SID)

Une **approche cohérente et globale des systèmes d'information européens à grande échelle** ainsi qu'une **supervision efficace de la protection des données** sont des éléments essentiels du succès de ces systèmes. Le nouveau cadre juridique prévu par le traité de Lisbonne et la suppression de la structure en piliers de la législation de l'UE devraient également servir d'outil pour fournir plus de **cohérence** entre les systèmes anciennement fondés sur la base juridique des premier et troisième piliers. Il est également nécessaire d'accroître la collaboration entre les organes de protection des données impliqués dans la supervision des systèmes.

Dans ce contexte, le CEPD a émis un avis sur l'initiative de la République française concernant une décision du Conseil sur l'utilisation des technologies de l'information à des fins douanières. Dans cet avis, le CEPD a souligné la nécessité d'assurer la plus grande cohérence possible entre les deux parties du SID, à savoir la partie régie par l'ancien premier

pilier et la partie régie par l'ancien troisième pilier. Le CEPD a appelé à accorder davantage d'attention, dans la proposition, aux **garanties spécifiques de protection des données,** en particulier en ce qui concerne la limitation volontaire de l'utilisation des données intégrées dans le SID.

Le CEPD a également appelé à ce qu'un **modèle de contrôle coordonné** soit inséré dans la proposition, ce qui assurerait, si nécessaire, une cohérence avec les autres instruments juridiques régissant l'établissement et/ou l'utilisation d'autres systèmes d'information à grande échelle, car ce modèle devrait également s'appliquer au SIS II et au VIS.

Le modèle de supervision a été un thème important des discussions au Conseil et au Parlement européen. La CEPD a investi beaucoup de temps et d'énergie pour plaider en faveur d'un modèle coordonné. Malheureusement, le Conseil a adopté un texte qui ne reflète pas totalement ce modèle. D'un autre côté, le texte donne un élan accru à une coopération étroite et efficace entre le CEPD et les autorités nationales de protection des données.

3.4. Vie privée et communications électroniques et technologie

3.4.1. Le CEPD et la directive «Vie privée et communications électroniques»

Au cours de l'année 2009, la directive 2002/58/CE concernant la vie privée et les communications électroniques, également appelée **directive «Vie privée et communications électroniques»,** est entrée dans la phase finale du processus de révision. L'adoption finale a eu lieu le 25 novembre 2009 ([10]). Ses nouvelles dispositions renforcent la protection de la vie privée et des données à caractère personnel de tous les Européens actifs dans un environnement en ligne. Parmi les améliorations les plus pertinentes, citons:

- la notification obligatoire des violations de la sécurité. Tout fournisseur de services de communications électroniques (par exemple un fournisseur de services internet) doit informer ses clients de toute violation de la sécurité susceptible de les toucher, par exemple la perte de données à caractère personnel pouvant avoir pour résultat une usurpation de l'identité, une fraude, une humiliation ou des dommages à la réputation;

- les nouvelles réglementations sur les cookies et les logiciels espions. Conformément à la nouvelle disposition, les utilisateurs devraient disposer de meilleures informations et de moyens plus faciles d'accepter ou de rejeter les cookies stockés sur leur terminal;

- l'amélioration du droit d'action contre les polluposteurs en donnant à toute personne négativement touchée par un pollupostage, notamment les fournisseurs de services internet, la possibilité d'attaquer les polluposteurs en justice;

- les dispositions renforçant les pouvoirs d'exécution des autorités de protection des données.

Tout au long du processus législatif et jusqu'à l'adoption finale, le CEPD a été totalement disponible pour conseiller les décideurs et les aider à définir les solutions politiques adéquates. Le CEPD a été particulièrement satisfait du cadre final relatif à la notification obligatoire des violations de la sécurité.

Dans son deuxième avis législatif, le CEPD a donné des conseils, entre autres, sur les principaux éléments du cadre juridique relatif à la notification des violations de la sécurité ([11]).

Le CEPD a salué la définition large des violations de la sécurité, et notamment de toute violation

([10]) Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 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 entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO L 337 du 18.12.2009, p. 11.

([11]) Deuxième avis du 9 janvier 2009 relatif au réexamen de 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 128 du 6.6.2009, p. 28.

Des traces personnelles des individus subsistent toujours après les communications électroniques.

conduisant à la destruction, à la perte, à la divulgation, etc., des données à caractère personnel transmises, stockées ou traitées en connexion avec le service. Comme critère de déclenchement (ou critère) de la notification, il a proposé que la notification aux individus soit obligatoire, si la violation des données est *susceptible d'avoir un effet négatif sur les données personnelles ou la vie privée*. Il a donné les raisons pour lesquelles cette norme était préférable aux autres normes proposées et a été ravi que cette préférence soit suivie. Il a également salué la décision de rendre les entités concernées responsables de l'évaluation du respect ou non du critère de déclenchement par la violation.

Malheureusement, le législateur n'a pas suivi la recommandation du CEPD de rendre cette disposition applicable à tous les responsables de traitement de données et a choisi de la limiter aux services de communications électroniques tels que les compagnies de télécommunications, les fournisseurs de services internet, les fournisseurs de messageries électroniques, etc.

La limitation de la portée a provoqué un débat animé entre le Parlement européen — qui était pour un champ d'application bien plus large — et le Conseil et la Commission, qui soutenaient une portée plus limitée. Si l'issue finale est insatisfaisante, le débat a poussé la Commission à exprimer son intention de rendre ce régime obligatoire pour tous les responsables de traitement de données dans un avenir proche.

La directive «Vie privée et communications électroniques» révisée autorise la Commission, en consultation avec les parties prenantes et le CEPD, à adopter des mesures d'application technique, à savoir des mesures détaillées sur la notification d'une violation de la sécurité, dans le cadre d'une procédure de comitologie. Cela garantira une mise en œuvre et une application cohérentes du cadre juridique en matière de violation de la sécurité dans toute l'UE, de manière à ce que les citoyens jouissent d'un niveau élevé égal de protection et que les fournisseurs de services ne soient pas étouffés par des exigences de notifications divergentes.

Le CEPD a organisé deux événements visant à partager expériences et meilleures pratiques. Ces initiatives devraient être utiles dans la future procédure de comitologie. Le premier événement a eu lieu en avril 2009. Il a été organisé dans le cadre de l'initiative de Londres et était réservé aux autorités de protection des données. Le deuxième événement, adressé au grand public, a eu lieu en octobre 2009 et était organisé conjointement avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

La directive «Vie privée et communications électroniques» a été adoptée en même temps que d'autres directives, dans le cadre du **«paquet télécom».**

Les dispositions relatives aux régimes de riposte graduée ou «approche des trois avertissements» incluses dans la directive 2002/22/CE concernant le service universel et les droits des utilisateurs ont soulevé des questions de protection des données et de la vie privée. Le CEPD a traité de ce sujet dans ses commentaires du 16 février 2009, confirmant son avis contre la surveillance systématique et proactive des utilisateurs de l'internet respectueux de la loi pour lutter contre les infractions présumées au droit d'auteur.

La technologie moderne permet de suivre en permanence les déplacements des conducteurs.

3.4.2. Systèmes de transport intelligents

Le CEPD a attiré une attention particulière sur l'innovation technologique dans le domaine des transports. Des «systèmes de transport intelligents» (STI) sont actuellement mis en place en Europe, en vue de réduire la circulation et de rendre les transports plus sûrs et plus propres. Les systèmes se basent généralement sur des technologies de localisation, telles que la localisation par satellite et la RFID. Le déploiement des STI en Europe a des implications considérables sur la vie privée, notamment parce que ces systèmes permettent de suivre un véhicule et de récolter toute une série de données relatives aux habitudes de conduite des usagers de la route européens.

Les «systèmes de transport intelligents» appliquent des technologies de l'information et de la communication (comme les satellites, les ordinateurs, les téléphones, etc.) aux infrastructures de transport et aux véhicules. Le système d'appel d'urgence «e-Call» et le système de péage électronique «e-Toll» en sont de bons exemples.

Dans ses commentaires sur le plan d'action de la Commission visant à accélérer et coordonner le déploiement des STI en Europe, le CEPD a souligné la nécessité de tenir dûment compte de la protection de la vie privée et des données, afin de garantir la viabilité des STI dans toute l'Europe.

Il a, en outre, prévenu la Commission des risques d'incohérences et de fragmentation dans ce déploiement si certains points n'étaient pas harmonisés au niveau de l'UE:

- il est nécessaire de préciser si les services STI seront fournis sur une base volontaire ou obligatoire, et, le cas échéant, de dire lesquels;
- il est essentiel de préciser les fonctions des différentes parties impliquées dans les STI pour déterminer qui est chargé de garantir le bon fonctionnement des systèmes d'un point de vue de protection des données — en d'autres termes, qui est le responsable du traitement des données;
- des garanties appropriées doivent être mises en œuvre par les responsables du traitement qui fournissent des services STI de manière à ce que les technologies de localisation ne soient pas intrusives. L'utilisation de ces dispositifs devrait être strictement limitée à ce qui est nécessaire pour atteindre leurs objectifs. Il faut garantir que les données de localisation ne seront pas dévoilées à des destinataires non autorisés;
- la vie privée et la protection des données doivent être prises en compte de manière précoce dans la conception de l'architecture

STI, le fonctionnement et la gestion des systèmes *(Privacy by Design);*

- les responsables du traitement des données doivent garantir que les utilisateurs sont bien informés des objectifs et de la manière dont le traitement des données s'effectue.

3.4.3. Application de la directive sur la conservation des données

La directive 2006/24/CE sur la conservation des données est un instrument de lutte contre le terrorisme et les autres infractions pénales graves qui oblige les fournisseurs de services de communications et les réseaux de communication à conserver les données relatives au trafic des communications. Elle a été adoptée il y a plusieurs années sous une pression politique intense et soulève des questions qui rendent son application difficile.

Un groupe d'experts rassemblant les intérêts des services répressifs, de l'industrie et des personnes concernées a dès lors été créé dans le but principal de fournir des orientations, par exemple sur la question de savoir à quels fournisseurs s'applique la directive vu l'environnement complexe des services de messagerie électronique, des fournisseurs de transit, des réseaux tiers, etc. Le CEPD a participé activement à ce groupe et a insisté pour que toute orientation respecte les principes de la législation en matière de protection des données.

Dans ce contexte, une question intéressante et difficile a été posée, à savoir quelle législation s'applique en cas de communications impliquant plus d'un État membre, par exemple dans le cas des communications mobiles internationales ou des communications internet transfrontalières. La question devient encore plus complexe lorsque le fournisseur stocke les données dans un autre État membre que celui où elles ont été générées. Le groupe entend publier ses conclusions dans le courant de 2010.

3.4.4. RFID

En mai 2009, la Commission européenne a adopté une recommandation sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence ([12]). Le CEPD a été fréquemment consulté par la Commission au cours de la préparation de la recommandation et la majorité de ses commentaires ont été repris.

La Commission européenne a ensuite créé un groupe de travail informel sur la mise en œuvre de la recommandation RFID et un représentant du groupe de l'article 29 (G29) a assisté à deux réunions de ce groupe en 2009. Parmi les sujets abordés par ce groupe, citons la nécessité de procéder à une étude d'impact sur la protection des données et de la vie privée (EIVP). Conformément au point 4 de la recommandation, un cadre de réalisation concernant cette évaluation sera soumis pour approbation au G29.

3.4.5. Participation au 7e PC

Riseptis

Le CEPD a rejoint le comité consultatif Riseptis (*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) ([13]) en tant qu'observateur. Ce groupe consultatif de recherche de haut niveau créé par la Commission européenne et composé d'éminents acteurs dans le domaine scientifique, industriel et politique, vise à fournir des orientations sur les défis politiques et de recherche dans le domaine de la sécurité et de la confiance dans la société de l'information. Le CEPD a joué un rôle actif dans les réunions du Riseptis qui se sont tenues en 2009 et a fourni des avis ciblés, notamment sur les questions de la législation applicable aux technologies futures et émergentes, les principes de responsabilisation et de responsabilité, ainsi que sur le concept de *Privacy by Design*.

([12]) Recommandation C(2009) 3200 final de la Commission du 12 mai 2009, disponible à l'adresse suivante: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

([13]) http://www.think-trust.eu/riseptis.html

Le rapport de Riseptis intitulé «Confiance dans la société de l'information», publié en octobre 2009, contient des recommandations sur plusieurs problématiques à l'heure où l'UE entre dans l'ère numérique.

Elles portent notamment sur les éléments suivants:

- la recherche interdisciplinaire, le développement et le déploiement technologiques;
- des initiatives visant à rassembler les acteurs technologiques, politiques, juridiques et socio-économiques et à les faire travailler à une société de l'information fiable;
- un cadre européen commun de gestion de l'identité et de l'authentification;
- la poursuite du développement du cadre juridique de l'UE en matière de protection des données et de respect de la vie privée;
- des initiatives à grande échelle impliquant les secteurs privé et public, qui tirent avantage des forces de l'Europe en ce qui concerne la communication, la recherche, les études juridiques et les valeurs sociétales;
- la coopération au niveau mondial pour promouvoir des normes ouvertes et des cadres fédérés.

Projets RDT de l'UE

À la suite de son document stratégique de mai 2008, le CEPD a également fourni un soutien ciblé et fait des commentaires sur une série de projets RDT de l'UE dans différents domaines, notamment les systèmes de transport intelligents, la biométrie, les systèmes de contrôle à distance et la santé en ligne.

3.5. Mondialisation

3.5.1. Implication dans les normes mondiales

De nombreux acteurs, notamment de la société civile et de l'industrie, demandent un cadre harmonisé transfrontalier de protection des données, permettant de garantir la sécurité juridique et de faciliter les flux de données dans un contexte international. Des mesures concrètes en vue de développer des normes internationales de protection des données ont été prises lors de la conférence internationale des commissaires à la protection des données et de la vie privée qui s'est tenue à Madrid en novembre 2009. La conférence a adopté une résolution saluant un projet de normes internationales de protection des données et de la vie privée. Ces normes constituent un premier pas vers un instrument international contraignant. Elles sont le résultat d'un travail préparatoire intensif sous la direction de l'autorité espagnole de protection des données, auquel le CEPD a également participé activement.

> Les normes incluent les principes essentiels de la protection des données. Si ces principes sont largement inspirés par la directive européenne sur la protection des données, ils prennent également en considération d'autres approches de la protection des données ([14]).

Au respect des principes d'équité, de nécessité, de proportionnalité et de transparence viennent s'ajouter des obligations de responsabilisation de la part des responsables du traitement des données, ainsi que la nécessité d'intégrer la notion de *Privacy by Design*. Les projets de normes prévoient également des droits d'accès et de rectification pour les personnes concernées ainsi que des possibilités de recours judiciaire et administratif.

3.5.2. Dossiers passagers et dialogue transatlantique

Les problématiques relatives à la protection des données figurent en bonne place à l'agenda des négociations entre l'UE et les États-Unis.

([14]) Telles que l'approche des pays de l'Organisation de coopération et de développement économiques (OCDE) et de l'Organisation de coopération économique Asie-Pacifique (OCEAP), qui diffère légèrement de celle de l'UE.

Un autre élément de la mondialisation est le dialogue transatlantique entre l'Union européenne et les États-Unis pour faciliter l'échange de données à caractère personnel. Les transferts de données ont la plupart du temps lieu pour lutter contre le terrorisme et les crimes graves, comme le montre l'accord sur le transfert des dossiers passagers au *Department of Homeland Security* américain (décision du Conseil du 23 juillet 2007). Le groupe de l'article 29 comme le CEPD ont exprimé leurs inquiétudes quant aux conditions dans lesquelles les dossiers passagers sont collectés, traités et stockés ([15]). En 2009, un sous-groupe du G29, auquel participe le CEPD, a suivi la mise en œuvre de cet accord sur les dossiers passagers et a soulevé toute une série de questions, notamment concernant l'accès étendu dont dispose l'administration américaine aux données traitées par les systèmes de réservation informatiques et l'absence d'examen du système par les autorités européennes.

Dans un contexte plus large, les États-Unis et l'UE négocient la conclusion d'un accord sur le partage d'informations dans le vaste domaine de la répression. Les négociations ont débouché sur plusieurs rapports du *groupe de contact à haut niveau,* sur lesquels le CEPD a émis un avis ([16]). En 2009, les discussions se sont concentrées sur des questions spécifiques pour lesquelles les parties n'étaient pas entièrement d'accord, et en particulier le droit des individus à un recours administratif *et* judiciaire. Les parties entendent prendre d'autres mesures en vue d'arriver à un accord dans le courant de 2010. Le CEPD a contribué à la consultation publique sur l'accord organisée par la Commission.

3.5.3. SWIFT: transfert de données financières aux autorités américaines

Le CEPD a suivi de près les développements concernant le transfert des données relatives aux transactions financières européennes au Trésor américain à des fins de lutte contre le terrorisme et son financement. Ceci représente un exemple clair de données à caractère personnel collectées par des entreprises commerciales, utilisées à des fins de répression au niveau mondial.

Lorsque SWIFT, le principal convoyeur de données financières, a modifié son architecture pour maintenir les données financières européennes sur le territoire européen, la Commission européenne a commencé à négocier un accord international avec les autorités américaines pour éviter d'interrompre leur accès à ces données. Le CEPD a été consulté et a émis des commentaires, qui ont été envoyés aux institutions concernées et présentés à la commission LIBE en septembre 2009.

Selon le CEPD, un accord international devrait respecter les éléments suivants:
- *les demandes de transferts de données sont licites et proportionnées, en particulier vu la nature intrusive de la proposition;*
- *des mécanismes de recours sont disponibles et peuvent être utilisés effectivement par les citoyens européens;*
- *le partage avec d'autres autorités nationales et d'autres pays est limité;*
- *les autorités indépendantes de contrôle de la protection des données peuvent exercer leur pouvoir de contrôle, notamment en examinant la mise en œuvre de l'accord.*

Un accord intérimaire a été signé en novembre 2009, mais en vertu des nouvelles dispositions du traité de Lisbonne, le Parlement européen a refusé son avis conforme. Au cours de 2010, le CEPD continuera de conseiller les institutions de l'UE afin de garantir le respect des normes européennes de protection des données à caractère personnel, en particulier en relation avec tout nouvel accord qui remplacera l'accord intérimaire.

([15]) Voir le rapport annuel 2008 du CEPD.

([16]) 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, JO C 128 du 6.6.2009, p. 1.

L'accès des pouvoirs publics aux transactions bancaires sera soumis à des conditions strictes.

3.5.4. Mesures restrictives concernant les terroristes présumés et certains pays tiers

Dans deux avis rendus en 2009, le CEPD a évoqué pour la première fois les «listes noires de terroristes». Ces instruments juridiques visent à lutter contre le terrorisme ou les violations des droits de l'homme en imposant des mesures restrictives — notamment le gel des actifs et les interdictions de voyager — à des personnes physiques ou morales suspectées d'avoir des liens avec des organisations terroristes et/ou certains gouvernements. La Commission européenne rédige et publie des «listes noires» de personnes soumises à ces mesures restrictives.

Dans plusieurs cas, la Cour de justice de l'Union européenne a réaffirmé que toutes les mesures prises par l'UE, même celles résultant de décisions de l'Organisation des Nations unies (ONU), devaient respecter les droits fondamentaux de l'UE, en particulier le droit à la défense et le droit d'être entendu. Il est à noter que la Cour a biffé de la liste certains individus soit parce qu'ils n'étaient pas en position de connaître la raison pour laquelle ils y figuraient, soit parce qu'ils étaient sur la liste depuis plusieurs années sans condamnation formelle ni enquête en cours.

Le CEPD s'est félicité des dernières propositions de la Commission visant à améliorer le respect des droits fondamentaux et reconnaissant explicitement l'applicabilité du règlement (CE) n° 45/2001 à ce domaine sensible d'un point de vue politique. Il a recommandé que:

- la qualité des données soit garantie en tenant compte des développements pertinents dans les enquêtes policières et de sécurité sur lesquelles se basent les listes, et en procédant à des révisions régulières des listes;
- les personnes figurant sur les listes soient dûment informées et aient le droit d'accéder aux données à caractère personnel les concernant;
- les restrictions et limitations nécessaires de ces droits soient clairement définies dans la législation, qu'elles soient prévues et proportionnées;
- les recours judiciaires, la responsabilité financière et la compensation adéquate soient garantis en cas de traitement illicite des données à caractère personnel.

Le CEPD s'est, pour la première fois, penché activement sur ce domaine sensible.

Le CEPD continuera à suivre les développements dans ce domaine à la fois en tant que conseiller des institutions européennes et en tant que superviseur du traitement de ces listes noires, notifié pour contrôle préalable par la Commission européenne à la fin de 2009.

3.6. Santé publique

L'UE a un programme ambitieux d'amélioration de la santé des citoyens dans la société de l'information et estime qu'il existe de grandes possibilités d'améliorer la santé des citoyens au niveau transfrontalier par le recours aux technologies de l'information. Il apparaît toutefois clairement que l'amélioration des soins de santé transfrontaliers grâce à l'utilisation des technologies de l'information a des implications importantes pour la protection des données à caractère personnel.

Depuis 2008, des initiatives concrètes dans ce domaine ont été adoptées ou proposées par la Commission. Celle-ci a publié une communication sur la télémédecine et une recommandation sur l'interopérabilité transfrontalière des systèmes de dossiers médicaux électroniques. Elle a également amélioré le système d'alerte rapide (SAR) et de réaction concernant les maladies contagieuses et a proposé une législation sur les droits des patients en matière de soins de santé transfrontaliers, de transplantation d'organes et de pharmacovigilance (détection et analyse des effets négatifs des médicaments).

Le CEPD s'est dit inquiet qu'en général, la plupart de ces textes évoquent à peine la protection des données. La question de la protection des données est évoquée et il est fait référence à la législation applicable en matière de protection des données, mais aucune mesure concrète n'est proposée permettant réellement d'assurer le respect des obligations en matière de protection des données et d'assurer que les États membres appliquent ces règles de manière cohérente. Aucune vision cohérente de la protection des données dans le secteur des soins de santé ne semble exister.

Cela peut s'expliquer en partie par le manque de conscience à la protection des données dans le secteur de la santé publique, tel que reflété au niveau européen par le manque d'information des départements responsables concernant l'existence du CEPD et leur obligation de le consulter. L'exemple le plus frappant à cet égard concerne la proposition sur la pharmacovigilance, qui ne fait aucune mention de la protection des données et n'a pas été envoyée au CEPD pour consultation.

Le CEPD a à maintes reprises souligné que les données de santé étaient considérées comme une catégorie d'informations personnelles sensibles et que le traitement de ces données était en principe interdit. Il existe des exceptions, notamment lorsqu'une personne est soumise à un diagnostic médical, mais ces exceptions doivent être appliquées de manière restrictive.

Dans son avis sur la pharmacovigilance, le CEPD a souligné le principe de nécessité et remis en cause la nécessité de traiter des données à caractère personnel dans la base de données européenne centralisée EudraVigilance.

Dans son avis sur la transplantation d'organes, le CEPD a précisé la notion d'«anonymisation». Il a expliqué que si la traçabilité des organes était garantie, ce qui signifie que le donneur peut toujours être retrouvé, les informations connexes ne pouvaient être considérées comme anonymes. Comme les propositions garantissaient la traçabilité et l'anonymat des informations en même temps, il fallait les adapter en mettant l'accent sur la confidentialité des informations plutôt que sur leur anonymat.

Le CEPD a à maintes reprises souligné que les règles en matière de protection des données n'étaient pas destinées à entraver une coopération efficace dans le domaine de la santé publique. Au contraire, les garanties de protection des données sont essentielles pour préserver la confiance dans la profession médicale et les services de santé en général.

La Cour européenne des droits de l'homme a jugé que «la protection des données à caractère personnel, en particulier des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et de la vie familiale garanti par» l'article 8 de la convention. Elle a ajouté que «le respect de la confidentialité des données relatives à la santé est [...] crucial non seulement [pour] respecter la vie privée d'un patient, mais aussi [pour] préserver sa confiance dans la profession médicale et dans les services de santé en général» ([17]).

Le CEPD s'est félicité des invitations reçues de la commission ENVI du Parlement européen, qui lui ont permis d'expliquer deux de ses avis (sur les soins de santé transfrontaliers et les transplantations d'organes). Il était également satisfait que ses propositions aient débouché sur l'adoption de plusieurs amendements par le Parlement européen, même si aucun des instruments juridiques proprement dits n'a encore été adopté.

Les activités dans le domaine de la santé publique ont poussé le CEPD à adopter une approche intégrée de ses fonctions consultatives et de supervision.

Les données à caractère personnel doivent-elles être traitées dans la base de données Eurovigilance?

([17]) Voir Cour européenne des droits de l'homme, 17 juillet 2008, *I contre Finlande* (appl. n° 20511/03), paragraphe 38.

La consultation sur les propositions concernant la pharmacovigilance a été associée à une analyse sur la base d'une notification en vue d'un contrôle préalable du système par l'Agence européenne des médicaments. Il en a été de même pour le développement du système d'alerte rapide et de réaction concernant les maladies contagieuses par la Commission et le Centre européen de prévention et de contrôle des maladies (ECDC). Le CEPD a fourni des commentaires informels sur la décision de la Commission concernée et a entamé une analyse du système après avoir reçu une notification en vue d'un contrôle préalable.

3.7. Accès du public et données à caractère personnel

3.7.1. Introduction

La relation complexe entre les règles européennes en matière d'accès du public aux documents et de protection des données occupe le CEPD depuis plusieurs années. En 2009, il a participé à la discussion sur la modification de la législation européenne sur l'accès du public aux documents et est intervenu dans des affaires en justice en la matière, notamment l'affaire *Bavarian Lager*. En outre, la première affaire portée devant le Tribunal de première instance contre une décision du CEPD relative à une réclamation portait sur ce sujet.

3.7.2. Modification de la législation européenne sur l'accès du public aux documents

Après avoir pris acte des discussions en cours au Parlement européen concernant la modification de la législation européenne sur l'accès du public aux documents, le CEPD a résumé les vues exprimées dans son avis du 30 juin 2008 dans des commentaires brefs. Le CEPD a souligné les conséquences négatives de certains des amendements déposés au Parlement pour la relation entre les deux droits. Le CEPD a été très satisfait que l'issue du vote en plénière ait pratiquement totalement reflété son approche.

Dans un communiqué de presse publié après le vote, le CEPD affirmait: «Ces amendements apportent de la clarté et évitent une application trop empressée des règles relatives à la protection des données dans ce domaine. Ils confirment que la protection des données ne fait pas obstacle à la divulgation d'informations personnelles dans les cas où la personne concernée n'a pas de motif légitime pour garder les données secrètes.»

Le CEPD a donné une explication orale de ses vues au groupe de travail du Conseil sur l'information. Malgré les efforts de la présidence suédoise en vue de faire passer la modification devant le Conseil au second semestre de 2009, la discussion sur la modification n'a pu réellement démarrer en raison d'un conflit de procédure entre la Commission et le Parlement, conflit qui n'est toujours pas résolu.

3.7.3. L'appel dans l'affaire *Bavarian Lager*

L'affaire *Bavarian Lager* concernait le refus par la Commission de divulguer cinq noms contenus dans un de ses documents. La Commission a interjeté appel contre l'arrêt du Tribunal de première instance du 8 novembre 2007, ce qui a débouché sur une audience le 16 juin 2009. Au cours de cette audience, le CEPD a plaidé en faveur du maintien de l'arrêt du Tribunal de première instance. Même si l'avocate générale Sharpston a également rejeté l'appel de la Commission dans son avis du 15 octobre 2009, elle ne partageait pas le raisonnement du Tribunal de première instance soutenu par le CEPD. Comme la conclusion de l'avocate générale se basait sur un raisonnement qui n'avait pas du tout été évoqué par les parties, le CEPD et la Commission ont demandé au tribunal de rouvrir la procédure orale.

3.7.4. Autres affaires judiciaires sur l'accès du public et la protection des données

L'affaire *Dennekamp* portée devant le Tribunal de première instance concernait le refus du Parlement de divulguer des documents mentionnant quels députés européens étaient également membres du régime de pension complémentaire. D'un point de vue juridique, l'affaire peut être considérée comme relevant du même chef d'accusation que l'affaire *Bavarian Lager*. Pour cette raison, le CEPD est intervenu dans l'affaire.

La toute première procédure judiciaire s'opposant à une décision du CEPD a été lancée par M^me^ Kitou le 3 avril 2009. Celle-ci contestait une décision du CEPD dans laquelle il avait conclu que les règles de protection des données ne constituaient pas un obstacle à la divulgation publique par la Commission, du fait qu'elle travaillait ou non à la Commission à certains moments.

Les deux affaires sont encore en cours au moment de l'impression du présent rapport annuel.

Deux autres affaires, qui sont toujours en cours, sont celles qui opposent M. Pachtitis à la Commission et à l'EPSO devant le Tribunal de première instance et le Tribunal de la fonction publique (TFP). La thématique de ces affaires est différente de celles évoquées plus haut, étant donné que le candidat souhaitait avoir accès à ses propres données à caractère personnel, ce que la Commission lui a refusé sur la base de la législation européenne sur l'accès du public aux documents. Dans les plaidoiries écrites et au cours de l'audience devant le TFP, qui a eu lieu le 1^er^ décembre 2009, le CEPD a affirmé que la demande d'accès devait être examinée au regard des règles de protection des données et que ces règles devaient être appliquées proactivement par la Commission.

Dans la discussion sur la modification des règles européennes en matière d'accès du public aux documents, le CEPD a affirmé que cette obligation devait être incluse dans le préambule du document modifié. Cette proposition a bénéficié du soutien du Parlement européen.

Le CEPD se consacre à l'étude de la relation complexe entre ces deux droits fondamentaux.

3.8. Autres questions diverses

3.8.1. Système d'information du marché intérieur

En 2009, le CEPD a continué de participer étroitement au développement du système d'information du marché intérieur (IMI), qui est peut-être l'exemple le plus frappant de coopération administrative grâce au partage d'informations, et qui constitue un instrument d'intégration européenne accrue. Le système IMI est devenu opérationnel — plus de 4 500 autorités compétentes étaient enregistrées dans ce système à la fin 2009 — et de nombreuses mesures ont été prises pour y inclure des garanties de la protection des données.

Le CEPD a salué ces efforts, tout en soulignant constamment l'importance d'un cadre plus global d'opération de l'IMI permettant de fournir une certitude juridique et un niveau plus élevé de protection des données — de préférence, sous la forme d'un règlement du Conseil et du Parlement.

3.8.2. Autres avis

Le CEPD a également émis des avis sur des sujets pour lesquels la protection des données n'était pas l'élément central, même s'il y avait un lien avec le traitement des données à caractère personnel. Il s'agissait notamment d'une proposition de directive du Conseil faisant obligation aux États membres de maintenir un niveau minimum de stocks de pétrole brut et/ou de produits pétroliers, d'une proposition de règlement du Conseil instituant un régime communautaire de contrôle afin d'assurer le respect des règles de la politique commune de la pêche et d'une recommandation pour un règlement du Conseil concernant la collecte d'informations statistiques par la Banque centrale européenne.

3.9. Un regard sur l'avenir

3.9.1. Développements technologiques

Comme mentionné dans le rapport annuel 2007 du CEPD, la société de l'information ne devrait plus être considérée comme un environnement parallèle et virtuel, mais de plus en plus comme un monde complexe et interactif qui s'imbrique dans le monde physique de l'individu. La convergence de ces deux mondes est facilitée par le nombre de

La société de l'information s'insinue dans tous les aspects du monde matériel de l'individu.

plus en plus important de ponts créés par l'utilisation innovante des technologies existantes et par le développement de technologies nouvelles et émergentes. Cette tendance est naturelle et positive et conduira en fin de compte à une intégration totale dans laquelle la société de l'information sera simplement une partie de la société.

Toutefois, la prolifération de ces ponts tend à brouiller les frontières entre des environnements qui ne sont pas nécessairement, pour le moment, régis par le même cadre juridique, et crée donc des incertitudes juridiques qui peuvent nuire à la confiance et au développement de la société de l'information.

Les exemples suivants illustrent ces ponts.

- ***CCTV «intelligente»:*** *ces systèmes sont souvent utilisés pour enquêter sur des incidents qui ont eu lieu dans le passé et sur les poursuites des infractions connexes qui ont suivi. Couplées à un logiciel de reconnaissance faciale et reliées à des bases de données privées ou publiques telles que les réseaux sociaux, les images de CCTV en temps réel (monde réel) pourraient être enrichies de données supplémentaires en ligne (monde numérique).*
- ***Internet des objets:*** *ce concept global est défini dans une communication de la Commission ([18]) publiée en juin 2009. Ces réseaux d'objets marqués interconnectés établiront clairement des liens entre la nature réelle de ces objets (par exemple localisation, situation, activités, comportement, propriété) et les informations en ligne qui les concernent, continuellement alimentées par un réseau de capteurs. Dans ce nouvel environnement, le long cycle de vie de certains objets marqués (par exemple pneus, lunettes) renforcera les liens en fournissant au fil du temps des informations encore plus précises sur les objets et leurs propriétaires.*
- ***Réfrigérateur intelligent:*** *cet exemple très souvent utilisé porte sur la relation entre les appareils ménagers et de cuisine et les fournisseurs en ligne. Même si un contrôle proactif de l'utilisation du réfrigérateur dans la maison est considéré comme inacceptable, le traitement des données générées par le réfrigérateur et communiquées à des fournisseurs en ligne pourrait être régi par différentes législations applicables.*
- ***Publicité comportementale:*** *le traitement et la corrélation d'une grande variété de données relatives au comportement en ligne des individus permettent de produire des profils précis qui peuvent être utilisés pour adapter les publicités à chaque individu. Les navigateurs internet et/ou les nouveaux appareils de communication fournissent des données de localisation et des schémas de mouvements associés à d'autres dispositifs, objets, personnes, magasins, etc., qui, ajoutés à leurs données sur leur comportement en ligne, peuvent aider à compléter les profils des utilisateurs.*

([18]) «L'internet des objets — Un plan d'action pour l'Europe», COM(2009) 278 final du 18 juin 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:FR:PDF

La convergence de ces deux mondes dans un espace continu pour l'individu a indubitablement créé de nouveaux défis pour le cadre juridique de l'UE en matière de respect de la vie privée et de protection des données. L'objectif est bien sûr clairement de réconcilier les environnements en ligne et hors ligne dans un seul environnement harmonisé ou au moins d'améliorer leur interopérabilité, afin de ne pas mettre en péril la confiance en cette ère numérique prometteuse.

3.9.2. Développements politiques et législatifs

Au moment de la mise sous presse de ce rapport annuel, des développements ont lieu (ou ont eu lieu) qui détermineront le contexte des politiques et des législations en 2010.

- *L'élément le plus important est l'entrée en vigueur du **traité de Lisbonne,** renforçant l'importance de la protection des données dans le cadre du traité et requérant une initiative législative.*
- *Le **programme de Stockholm** met un accent important sur la protection des données. Il souligne l'importance de la protection des droits fondamentaux dans la société de l'information et il mentionne la protection des données comme condition préalable à l'échange d'informations dans le but de garantir la sécurité de la société.*
- *La **nouvelle Commission** entrée en fonction avait de grandes ambitions en matière de protection des données et de la vie privée. La nouvelle commissaire chargée des droits fondamentaux et de la justice continue de considérer le cadre global de protection des données comme l'une de ses priorités principales.*
- *La nouvelle Commission travaille sur l'**agenda numérique de l'Europe,** pour lequel **le respect de la vie privée et la protection des données sont des conditions préalables nécessaires,** avec un accent prononcé, par exemple, sur la notion de* Privacy by Design.
- *On assiste également à des développements importants qui permettront à l'UE et à ses États membres d'aborder plus efficacement la **dimension externe de la protection des données,** non seulement en relation avec les États-Unis, en tant qu'acteur le plus important dans l'échange de données, mais aussi à une plus grande échelle par le développement de normes mondiales.*

Ces développements se feront, à l'évidence, plus tangibles lorsque la nouvelle Commission détaillera ses ambitions. Le programme législatif et de travail 2010 de la nouvelle Commission et son plan d'action pour la mise en œuvre du programme de Stockholm seront des documents importants à cet égard. Le CEPD est bien sûr particulièrement intéressé par le suivi de la consultation publique sur le futur cadre de protection des données.

Les autres domaines dans lesquels de nouveaux développements devraient avoir un impact sur le traitement des données à caractère personnel comprennent différents instruments européens dans les domaines de la santé publique, de la coopération fiscale, du transport (y compris les nouveaux développements en ce qui concerne le contrôle des voitures) et du projet e-Justice.

3.9.3. Priorités pour 2010

Le CEPD établira ses priorités pour 2010 en fonction des développements spécifiques au cours de l'année et poursuivra la direction de sa politique consultative de 2009. Les priorités seront établies dans l'inventaire 2010, qui sera publié à l'issue du programme législatif et de travail 2010 de la Commission, attendu pour la fin de mars 2010.

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 dédié à la protection des données à caractère personnel, agissant dans le cadre de ladite directive ([19]). 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 aux activités du groupe. Le CEPD estime qu'il s'agit d'un forum très important 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 2009, le groupe de travail a concentré ses activités sur les éléments définis dans son programme de travail 2008-2009, à savoir:

- 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 de l'article 29.

([19]) 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, du Liechtenstein et de la Norvège [partenaires de l'Espace économique européen (EEE)] sont représentées en tant qu'observatrices.

Le groupe a adopté plusieurs documents à cet égard:

- **meilleure mise en œuvre de la directive 95/46/CE:** contribution conjointe sur l'avenir de la protection de la vie privée, en réponse à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel (WP168);

- **transferts internationaux:** avis 3/2009 concernant le projet de décision de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants de données établis dans des pays tiers en vertu de la directive 95/46/CE (responsable vers sous-traitant) (WP161); avis sur le niveau de protection en Andorre (WP166) et en Israël (WP165);

- **nouvelles technologies:** avis sur les réseaux sociaux en ligne (WP163); avis concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «Vie privée et communications électroniques») (WP159).

Le groupe a réagi aux développements dans le domaine des **nouvelles technologies** et il a suivi la mise en œuvre de son avis sur les **moteurs de recherche** adopté en 2008 en organisant une audition des fournisseurs de moteurs de recherche.

Le groupe et le CEPD ont coopéré étroitement sur des questions relatives aux nouveaux défis dans le domaine de la protection des données. En plus d'une étroite collaboration concernant **l'avenir du cadre de protection des données,** le groupe et le CEPD ont rédigé une réponse commune à la consultation de la Commission sur «l'**impact de l'utilisation des scanners corporels** dans le domaine de la sécurité aérienne sur les droits de l'homme, la vie privée, la dignité personnelle, la santé et la protection des données».

Le CEPD coopère également avec les autorités nationales de contrôle dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes informations utiles, en leur demandant ou leur fournissant une aide à l'exécution de leurs fonctions [article 46, point f), i), du règlement]. Cette coopération se fait cas par cas.

La coopération directe avec les autorités nationales devient encore plus pertinente dans le contexte du développement de grands systèmes internationaux tels Eurodac, qui requièrent une approche coordonnée du contrôle (voir le point 4.3).

4.2. Groupe «Protection des données» du Conseil

Ces dernières années, sous diverses présidences, le groupe «Protection des données» du Conseil a permis aux États membres de discuter des questions de protection des données dans le cadre de l'ancien «premier pilier». En 2009, le groupe de travail s'est réuni une fois, sous la présidence tchèque. Le CEPD en a profité pour présenter aux représentants des États membres un aperçu de ses activités.

Vu l'absence d'initiatives législatives générales sur la protection des données dans ce domaine, le groupe n'a pas atteint son plein potentiel. Toutefois, en agissant en tant que plate-forme d'échange d'informations, et en fournissant son expertise de manière proactive, il pourrait jouer un rôle constructif pour contribuer à développer un cadre juridique global de protection des données — un rôle que saluerait le CEPD.

La présidence espagnole a également prévu une réunion du groupe en mars 2010.

4.3. Supervision coordonnée d'Eurodac

La supervision efficace d'Eurodac repose sur une coopération étroite entre les autorités nationales de protection des données et le CEPD. Le groupe de coordination du contrôle d'Eurodac (ci-après «le groupe») est composé de représentants des autorités nationales chargées de la protection des données et du CEPD, et s'est réuni trois fois en 2009.

Deuxième rapport d'inspection

L'une des principales réalisations du groupe cette année a été l'adoption, en juin, de son deuxième rapport d'inspection. Le rapport présente à la fois les résultats et les recommandations basés sur les réponses obtenues de tous les États membres. Un des objectifs de cet exercice est de contribuer efficacement à la révision en cours du cadre d'Eurodac et de Dublin (voir aussi le point 3.3.2).

Les deux principales questions examinées par le groupe étaient le droit d'information pour les demandeurs d'asile et les méthodes d'évaluation de l'âge des jeunes demandeurs d'asile. Le rapport a été envoyé aux principaux acteurs institutionnels de l'UE, ainsi qu'aux organisations internationales et organisations non gouvernementales (ONG) concernées par l'asile et les questions d'immigration.

Le droit d'information

Sans information claire et accessible, les personnes soumises au système Eurodac ne sont pas en mesure d'exercer leur droit à la protection des données.

L'inspection a montré que les informations fournies aux demandeurs d'asile sur leurs droits et l'utilisation de leurs données tendaient à être incomplètes, en particulier celles concernant les conséquences de la prise d'empreintes et le droit d'accès et de rectification de leurs données. Les informations fournies varient fortement entre les États membres et des différences significatives ont été observées concernant les pratiques à l'égard des demandeurs d'asile et des immigrés clandestins.

En conséquence, le rapport a recommandé que les États membres améliorent la qualité des informations qu'ils fournissent sur la protection des données. Ces informations devraient couvrir les droits d'accès et de rectification ainsi que la procédure régissant l'exercice de ces droits. En outre, les autorités d'asile devraient garantir que les informations seront fournies de manière cohérente aux demandeurs d'asile et aux immigrés clandestins, et ce de façon claire et facilement intelligible. Un accent particulier devrait être placé sur la garantie de la visibilité et de l'accessibilité des informations. En outre, les États membres devraient promouvoir la coopération et le partage des expériences entre les autorités nationales compétentes, en encourageant un groupe de travail à étudier cette question et à développer ultérieurement des pratiques harmonisées.

Évaluation de l'âge des demandeurs d'asile

Le règlement Eurodac prévoit que les empreintes digitales doivent être relevées sur les enfants de 14 ans au moins. Il est souvent problématique de déterminer l'âge d'un enfant qui ne possède aucune pièce d'identité fiable, et différentes méthodes sont donc utilisées au niveau national.

L'inspection effectuée par le groupe s'est concentrée à la fois sur les méthodes d'évaluation de l'âge des demandeurs d'asile (notamment des examens médicaux intrusifs) et sur la procédure des tests.

L'une des conclusions était que les méthodes de détermination de l'âge des demandeurs d'asile devraient être clairement définies et accessibles au public. Il a été suggéré que dans un souci d'harmonisation, la Commission procède à une évaluation globale (y compris des aspects médicaux et éthiques) de la fiabilité des diverses méthodes d'évaluation de l'âge dans les États membres.

En outre, le demandeur d'asile doit avoir le droit de demander, sans frais supplémentaires, un deuxième avis sur les résultats des tests médicaux et des conclusions qui s'imposent. Les autorités d'asile doivent tenir compte de la marge d'erreur résultant de l'utilisation de certains examens médicaux lorsqu'elles prennent une décision quant au statut juridique du demandeur d'asile.

4.4. Troisième pilier

Le CEPD a poursuivi sa coopération avec les autorités de contrôle communes (ACC) de Schengen, d'Europol, d'Eurojust et du système d'information douanier, ainsi que du groupe de travail «Police et justice» (GTPJ) établi par la conférence européenne des commissaires à la protection des données pour contrôler et agir en fonction des développements relatifs à la protection des données dans le domaine de la répression.

Les travaux avec les ACC se sont concentrés sur l'échange d'informations et la stimulation de la cohérence et des améliorations dans le contrôle de la protection des données, en particulier au vu de l'entrée en vigueur du traité de Lisbonne. Le GTPJ peut être considéré comme un complément informel au groupe de l'article 29 dans les domaines pour lesquels ce dernier n'est pas compétent, et en particulier ceux relevant de l'ancien «troisième pilier». En tant que membre du GTPJ, le CEPD a pris part activement à ses activités. Il a notamment:

- contribué au débat sur le programme de Stockholm;
- évalué l'impact de la décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire, en se concentrant particulièrement sur les

manières de garantir une approche harmonisée de la mise en œuvre au niveau national;

- suivi la mise en œuvre de la convention sur la cybercriminalité du Conseil de l'Europe, le premier traité international définissant une politique commune de protection de la société face aux crimes commis sur l'internet ou d'autres réseaux informatiques;

- exprimé sa profonde inquiétude, en accord avec son avis, vis-à-vis de la proposition de la Commission d'autoriser l'accès à Eurodac à des fins répressives;

- compilé un registre de coopération et de supervision dans le domaine de la répression dans l'UE, qui a ensuite été adopté par la conférence européenne;

- contrôlé et amélioré les accords bilatéraux et multilatéraux en vigueur entre les pays européens et non européens dans le domaine de la coopération policière et judiciaire en matière pénale, notamment la lutte contre le terrorisme;

- suivi les développements de l'accord international avec les États-Unis sur le transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme, ainsi que le débat plus large sur l'établissement de principes transatlantiques de protection des données;

- contribué à un document conjoint sur l'avenir de la protection des données en Europe, en réponse à une consultation publique lancée par la Commission européenne.

Pour garantir la cohérence au sein des autorités européennes de protection des données, le GTPJ a collaboré étroitement avec le groupe de l'article 29 et a fait référence aux positions adoptées par le CEPD.

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. **La conférence européenne des commissaires à la protection des données s'est tenue à Édimbourg les 23 et 24 avril 2009.**

Cette conférence s'est concentrée sur la nécessité de **revoir le cadre européen de protection des données.** Quatre sessions ont été organisées sur ce thème:

- Présentation d'un projet de rapport par RAND Europe, commandé par l'Information Commissioner's Office britannique, intitulé «Révision de la directive européenne sur la protection des données», qui a fait l'objet de commentaires de la part du CEPD.

- Avons-nous besoin de réformes? Autres avis sur les forces et faiblesses de la directive 95/46/CE;

- Que pourrait apporter la réglementation aux individus, à la société et aux législateurs?

- Le contexte international de la réglementation.

Une déclaration «sur l'initiative et l'avenir de la protection des données en Europe» a été adoptée par la conférence, soulignant le rôle des autorités de protection des données dans ce débat. La conférence a également adopté une résolution sur les accords bilatéraux entre les États membres de l'UE et les pays tiers dans le domaine de la coopération policière et judiciaire en matière pénale.

La conférence a également fourni l'occasion de rendre compte des rencontres semestrielles de l'atelier de traitement des dossiers, auxquelles les membres des autorités européennes de protection des données participent afin d'échanger leurs idées en matière de bonnes pratiques. En 2009, les ateliers ont eu lieu à Prague (République tchèque) et à Limassol (Chypre). Le prochain atelier aura lieu à Bruxelles au printemps 2010.

La prochaine conférence européenne sera organisée par l'autorité tchèque de protection des données à Prague les 29 et 30 avril 2010.

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

Peter Hustinx s'exprimant lors de la conférence internationale des commissaires à la protection des données (Madrid, du 4 au 6 novembre 2009).

de la région Asie-Pacifique, se réunissent tous les ans à l'automne depuis plusieurs années. Cette année, la **conférence internationale des commissaires à la protection des données a été organisée par l'autorité espagnole de protection des données et s'est tenue à Madrid du 4 au 6 novembre 2009.** Elle a attiré un bon millier de participants, un record. Son thème principal était le suivant: «La vie privée, aujourd'hui, c'est demain».

Plusieurs sessions plénières ont été organisées pour examiner les questions suivantes:

- Une société surveillée? À la recherche de l'équilibre entre la sécurité et le droit à la vie privée
- Quo vadis internet?
- Droit à la vie privée et responsabilité de l'entreprise
- Protéger le droit à la vie privée des mineurs: une mission prioritaire
- *Privacy by Design* (prise en compte de l'impératif de protection de la vie privée dès la conception)
- Vers une régulation globale du droit à la vie privée: propositions et stratégies

La protection des données en tant qu'élément stratégique des activités et des transferts commerciaux et internationaux de données à l'ère de la mondialisation était l'un des points essentiels de la conférence. Cette conférence a été une occasion d'observer une demande croissante des acteurs, y compris la société civile et l'industrie, pour un cadre harmonisé de protection des données au-delà des frontières. C'est dans cet esprit que la conférence a adopté une résolution saluant le projet de normes internationales pour la protection des données et de la vie privée. Ces normes sont le résultat d'un an de travail préparatoire coordonné par l'autorité espagnole et représentent un premier pas vers un instrument législatif international.

Les systèmes de surveillance sont une autre question qui a été discutée en profondeur à Madrid, en particulier ceux basés sur les aspects du corps humain, par exemple la biométrie, dont l'utilisation s'étend à différents domaines de la vie quotidienne.

Le contrôleur et son adjoint ont tous deux participé à la conférence. Le premier a présidé la session parallèle «Détermination de la législation applicable dans le monde de la globalisation» et le second est intervenu dans la session parallèle «Avez-vous un droit à la vie privée à votre poste de travail?».

La prochaine conférence aura lieu à Jérusalem du 27 au 29 octobre 2010.

4.7. L'initiative de Londres

Une déclaration intitulée «Communiquer sur la protection des données et la rendre plus effective», qui a reçu le soutien général d'autorités de protection des données du monde entier, a été présentée lors de la 28e 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 [Commission nationale de l'informatique et des libertés (CNIL)], du commissaire à l'information du Royaume-Uni (Information Commissioner) et du CEPD. Étant un des principaux architectes 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 ([20]).

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, la planification stratégique et la gestion des autorités de protection des données.

En avril 2009, le CEPD a organisé à Bruxelles pour les autorités de protection des données un atelier destiné à un échange des meilleures pratiques pour «répondre aux violations de la sécurité». Cet atelier fermé a également servi de base à un séminaire avec d'autres acteurs sur le sujet, organisé par le CEPD en collaboration avec l'Agence européenne chargée de la sécurité des réseaux et de l'information, qui a eu lieu au Parlement européen en octobre 2009.

4.8. Organisations internationales

En novembre 2009, le CEPD et l'Institut universitaire européen (IUE) ont entamé les préparatifs en vue d'un troisième atelier sur la protection des données dans les organisations internationales, qui aura lieu au printemps 2010 à Florence.

À la suite de la résolution sur la protection des données et les organisations internationales adoptée en 2003 lors de la conférence internationale de Sydney ([21]), le CEPD, avec le Conseil de l'Europe, l'OCDE et l'Office européen des brevets, a organisé deux ateliers à Genève (2005) et Munich (2007). Les organisations internationales qui ne possèdent pas de législation nationale ne disposent souvent pas d'un cadre juridique de protection des données. Ces événements ont mis en évidence leur intérêt croissant pour la protection des données à caractère personnel et la garantie du respect des règles en leur sein.

Au cours de ce troisième atelier, le CEPD entend concentrer le débat sur les questions suivantes:

- la gouvernance de la protection des données dans les organisations internationales;
- le respect des règles en pratique, notamment dans la gestion des données relatives aux ressources humaines;
- les défis technologiques et les mesures de sécurité connexes;
- l'utilisation de la biométrie aux frontières et à des fins de sécurité intérieure.

([20]) Voir le rapport annuel 2006, points 4.5 et 5.1.

([21]) http://www.privacyconference2008.org/adopted_resolutions/5-SYDNEY2003/SYDNEY-EN4.pdf

5

COMMUNICATION

5.1. Introduction

L'information et la communication jouent un rôle essentiel pour assurer la visibilité des principales activités du CEPD, mieux sensibiliser au 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 à l'échelle de l'UE. Les premières années qui ont suivi la création de l'institution ont été principalement consacrées à cet objectif, ce qui s'est généralement avéré rentable en termes d'accroissement de la visibilité. Les indicateurs comme le nombre accru de demandes d'information soumises par les citoyens de l'UE, le nombre de requêtes des médias, le nombre d'abonnés à la newsletter, ainsi que le nombre d'invitations à venir s'exprimer à des conférences et le trafic sur le site internet montrent bien que le CEPD est devenu un point de référence pour les questions de protection des données.

La visibilité accrue du CEPD dans le paysage institutionnel présente une pertinence particulière 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 de 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 dans le domaine de la sécurité et de la justice.

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.

En 2009, les activités ont été principalement destinées à améliorer et développer les outils d'information et de communication aménagés au cours des premières années de l'institution, en vue de communiquer plus efficacement et d'en étendre la portée à l'administration de l'UE et au grand public.

Le contrôleur et le contrôleur adjoint ont consacré beaucoup de temps et d'efforts pour expliquer leur mission et sensibiliser le public à la protection des données. Lors de différents discours au cours de l'année, ils ont abordé plusieurs questions spécifiques (voir annexe G).

5.2. Caractéristiques de la communication

La politique de communication du CEPD doit être conçue en fonction de caractéristiques particulières pertinentes du point de vue de l'âge, de la taille et des compétences 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 européens, 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 contribue toutefois lui aussi à mieux se faire connaître du grand public, notamment grâce à un certain nombre d'outils de communication (site internet, newsletter 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. S'agissant des outils d'information et de communication visant toutes sortes de public, il convient de communiquer dans un style clair et intelligible qui évite tout jargon inutile. Des efforts constants sont donc fournis dans ce sens, qui visent 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.

5.3. Relations avec les médias

Le CEPD doit être aussi accessible que possible pour les journalistes de façon à ce que le public puisse suivre son travail. Il informe régulièrement les médias au moyen de communiqués de presse, d'interviews, de discussions de fond et de conférences de presse. La gestion fréquente des demandes formulées par les médias permet de renforcer ses contacts réguliers avec ceux-ci.

En 2009, le service de presse a publié 14 **communiqués de presse.** La plupart concernaient de nouveaux avis législatifs présentant un intérêt particulier pour le public. Ces questions couvrent notamment la révision de la directive «Vie privée et communications électroniques», l'accès du public aux documents de l'UE, le nouveau programme de Stockholm dans le domaine de la justice et des affaires intérieures, les systèmes de transport intelligents dans le transport routier, l'accès des services répressifs à Eurodac et la nouvelle agence pour les systèmes informatiques à grande échelle.

Les communiqués de presse sont publiés sur le site internet du CEPD et dans la base de données des communiqués de presse de la Commission européenne (RAPID) en anglais et en français. Ils sont distribués sur un réseau régulièrement mis à jour de journalistes et de parties intéressées. Les informations fournies dans les communiqués de presse contribuent généralement à la production d'une couverture médiatique importante, car ils sont souvent repris par la presse générale et spécialisée. Ils sont également fréquemment publiés sur des sites internet institutionnels et non institutionnels, notamment ceux des institutions et organes de l'UE, des ONG, des institutions académiques et des entreprises de technologies de l'information.

Peter Hustinx répondant aux questions d'un journaliste.

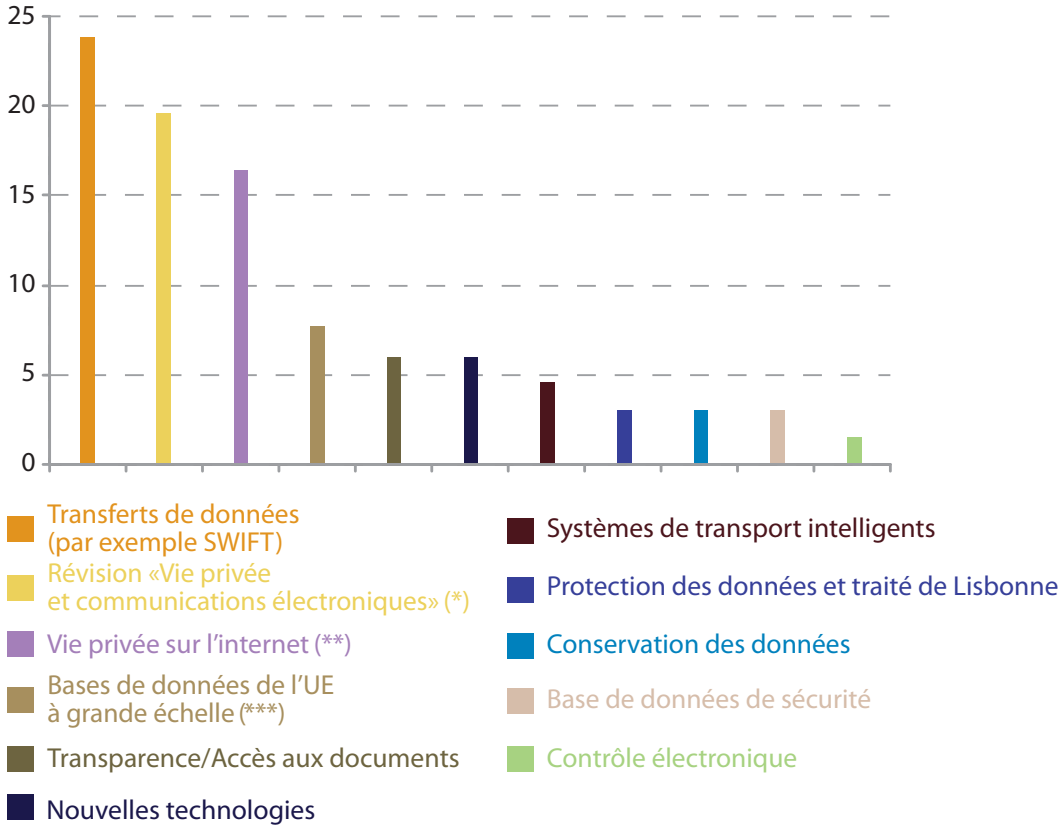
En 2009, le CEPD a donné quelque 20 **interviews** à des journalistes de la presse écrite, de la radiotélévision et des médias électroniques en Europe, un grand nombre de demandes émanant de la presse allemande, autrichienne, néerlandaise et belge. Cela a donné lieu à de nombreux articles dans la presse nationale, internationale et européenne, dans des publications et sur des sites internet spécialisés dans les technologies de l'information ainsi qu'à des interviews à la radio et à la télévision (par exemple la chaîne de télévision franco-allemande ARTE, la radio néerlandaise, les télévisions suédoise et néerlandaise). Les interviews ont abordé des questions horizontales comme la sécurité des données européennes, les tendances vers une société de surveillance et les défis actuels et à venir dans le domaine de la protection de la vie privée et des données. Elles ont également abordé des questions plus ciblées, notamment l'accord SWIFT entre l'UE et les États-Unis, les passeports biométriques et les bases de données et d'empreintes, la nouvelle exigence en matière de notification des violations des données dans la directive révisée «Vie privée et communications électroniques» et l'impact du traité de Lisbonne sur la protection des données.

Les demandes formulées par les médias parviennent régulièrement au CEPD et comprennent généralement des demandes de commentaires et des demandes de clarification ou d'information. En 2009, l'attention médiatique s'est principalement concentrée sur les questions de transferts de données (par exemple le débat sur un nouvel accord SWIFT), la révision de la directive «Vie privée et communications électroniques» (en particulier la nouvelle disposition sur les notifications obligatoires des violations de sécurité), les questions de vie privée sur l'internet, notamment les moteurs de recherche, les nouvelles applications en ligne et les nouveaux réseaux sociaux, et les bases de données à grande échelle de l'UE. L'accès aux documents de l'UE et aux nouvelles technologies (comme la RFID et l'informatique dématérialisée) a également été une question d'intérêt pour la presse.

5.4. Demandes d'informations et de conseils

Le nombre de demandes d'information ou d'aide soumises par les citoyens est resté assez stable en 2009 (174 demandes, contre 180 en 2008). 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 de l'information (cabinets juridiques, consultants, groupes de pression, ONG, associations, universités, etc.) aux citoyens souhaitant obtenir plus d'informations sur les questions relatives à la protection de la vie privée ou qui demandent une assistance pour résoudre les problèmes auxquels ils sont confrontés dans ce domaine. Ces demandes arrivent

Principaux sujets ayant fait l'objet de demandes par la presse en 2009



(*) Y compris la nouvelle disposition sur les failles de sécurité.

(**) Y compris les moteurs de recherche, les nouvelles applications en ligne et les réseaux sociaux.

(***) Principalement Eurodac, CIS et VIS.

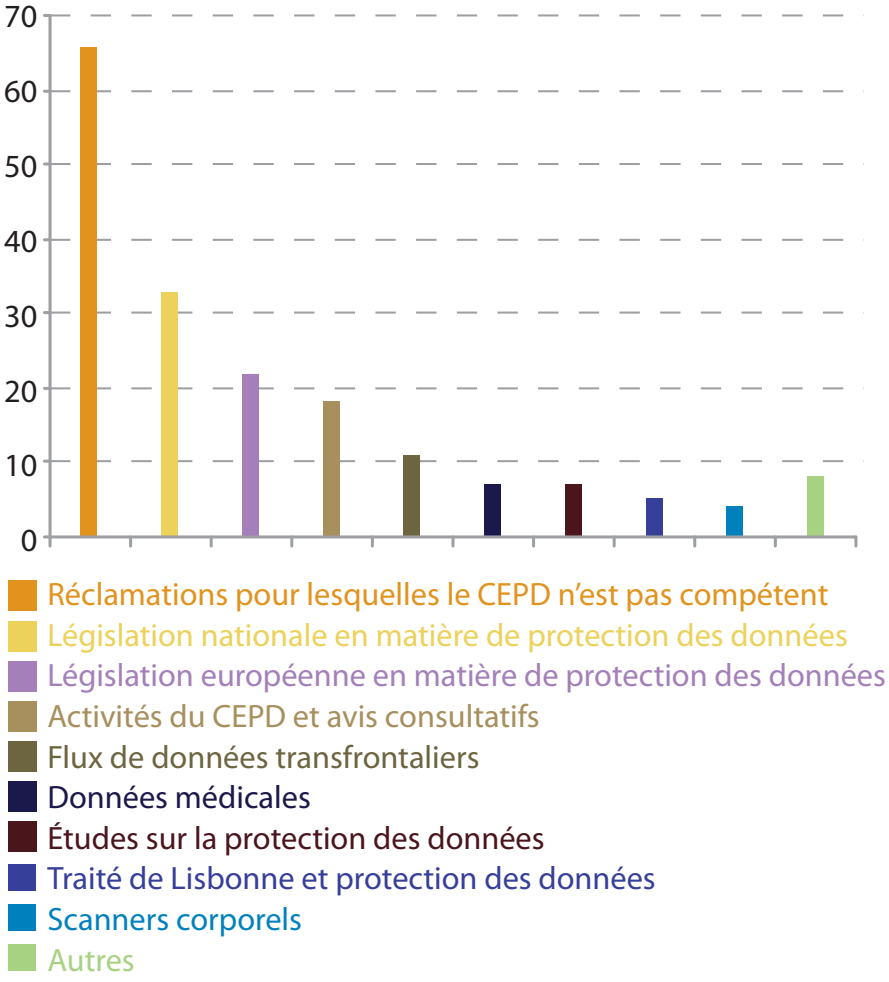
essentiellement dans la boîte électronique fonctionnelle du CEPD.

La première catégorie de demandes reçues en 2009 concerne les réclamations des citoyens de l'UE pour lesquelles le CEPD n'est pas compétent. Elles portaient la plupart du temps sur des violations présumées de la protection des données par les entreprises nationales ou les autorités publiques, les sites internet non européens ou les réseaux sociaux. D'autres concernaient une violation présumée de la vie privée au cours d'une procédure judiciaire et une demande d'appel contre un jugement émanant d'une autorité nationale de protection des données. Comme ces types de réclamations ne relèvent pas de la compétence du CEPD, une réponse est envoyée précisant le mandat du CEPD et conseillant au plaignant de s'adresser à l'autorité compétente, en général l'autorité nationale de protection des données de l'État membre concerné.

La deuxième catégorie de demandes reçues en 2009 concerne la législation en matière de protection des données dans les États membres de l'UE et/ou sa mise en œuvre. Dans ces dossiers, le CEPD conseille à la personne concernée de contacter l'autorité de protection des données (APD) concernée et, le cas échéant, l'unité de protection des données de la Commission européenne.

Les autres catégories de demandes d'informations relevaient la plupart du temps de la compétence du CEPD et ont donc reçu des réponses sur le fond. Il s'agissait notamment de demandes relatives à la législation européenne en matière de protection des données, aux activités du CEPD, aux flux transfrontaliers de données, aux nouvelles dispositions du traité de Lisbonne en matière de protection des données et aux questions de protection des données concernant l'utilisation des scanners corporels dans les aéroports.

Principaux domaines ayant fait l'objet de demandes d'information de la part du public en 2009



5.5. 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 dans les domaines du droit européen, de la protection des données et/ou de la sécurité des technologies de l'information. Ainsi, en octobre 2009, le bureau du CEPD a accueilli un groupe d'étudiants en droit international et européen de l'université de Grenoble, en France, pour leur présenter ses fonctions et ses activités et discuter des questions de protection des données en connexion avec la lutte contre le terrorisme. Il y a eu aussi d'autres groupes de visiteurs composés d'étudiants autrichiens de Master of Business Administration (MBA) en administration publique et d'étudiants de l'université de Tilburg aux Pays-Bas.

Pour atteindre un public plus jeune, l'office du CEPD a également accueilli un groupe d'étudiants autrichiens de l'enseignement secondaire, avec lesquels les membres du personnel ont évoqué des questions de protection des données présentant un intérêt pour eux, comme les réseaux sociaux en ligne et la protection des mineurs sur l'internet.

5.6. Outils d'information en ligne

Site internet

Le site internet reste l'outil de communication et d'information le plus important du CEPD. Il est mis à jour pratiquement tous les jours. C'est aussi sur le site que les visiteurs peuvent accéder aux documents élaborés dans le cadre des activités du CEPD (par exemple avis relatifs à des contrôles préalables et propositions d'actes législatifs européens, priorités de travail, publications, discours et contribu-

tions écrites, communiqués de presse, newsletters, informations sur les événements).

Évolution du contenu

En 2009, hormis une mise à jour pour refléter la désignation du contrôleur et du contrôleur adjoint pour leur deuxième mandat, de nouveaux outils d'information ont été publiés pour répondre davantage aux attentes des visiteurs et permettre une meilleure compréhension des activités du CEPD. Parmi ces améliorations, la publication d'un glossaire de termes relatifs à la protection des données à caractère personnel et d'une section «Questions-réponses».

Une mise à jour en profondeur de l'ensemble des pages du site internet a également été réalisée avant l'introduction d'une version allemande du site courant 2010, en plus de la version française et de la version anglaise. Le développement d'une section «Foire aux questions» est également en cours d'élaboration afin de fournir des réponses ciblées aux différents profils et publics (par exemple personnel de l'UE, visiteurs, candidats aux postes vacants dans les institutions et organes de l'UE).

D'autres améliorations du site internet sont prévues et comporteront l'introduction d'un formulaire de réclamation en ligne, le développement du registre des notifications et une révision de la page d'accueil afin de donner plus de visibilité aux dernières actualités relatives aux activités du CEPD.

Évolutions techniques et trafic

Dans le cadre des efforts continus pour rehausser la performance du site internet, de nombreux éléments, parfois moins visibles que d'autres, ont été améliorés en 2009 (par exemple l'outil de recherche avancée).

Une analyse des données sur le trafic et la navigation montre que le site internet a accueilli au total 92 884 visiteurs uniques en 2009, dont plus de 8 000 par mois en janvier, mars, avril, octobre et novembre. Après la page d'accueil, les pages le plus souvent consultées ont été les rubriques «Contact», «Supervision» et «Consultation», tandis que les pages «Actualités» et «Événements» étaient également populaires. Les statistiques montrent également que la plupart des visiteurs accèdent au site via une adresse directe, un onglet, un lien dans un courrier électronique ou un lien sur un autre site (portail Europa ou site internet d'une autorité nationale de protection des données). Les liens à partir des moteurs de recherche sont utilisés par un nombre très restreint de visiteurs. Ces chiffres nous font penser que le site internet du CEPD est consulté par un noyau de visiteurs réguliers qui ont confiance en son contenu.

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 internet. 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 internet du CEPD. Une fonction d'abonnement automatique figure sur la page concernée.

Cinq numéros de la newsletter du CEPD ont été publiés en 2009, soit en moyenne un tous les deux mois. La newsletter est publiée en anglais et en français, et une version allemande devrait voir le jour dans le courant de 2010.

Le nombre d'abonnés est passé de 880 personnes à la fin de 2008 à environ 1 200 à la fin de 2009. 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 l'augmentation régulière et importante du nombre d'abonnés, une nouvelle version de la newsletter, plus conviviale et mise à jour, s'est révélée nécessaire, ainsi qu'une structure révisée plus accessible. La première édition de la nouvelle version de la newsletter a été publiée en octobre 2009.

5.7. Publications

Rapport annuel

Le rapport annuel constitue la principale publication du CEPD. 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 l'UE 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 à caractère personnel au niveau de l'UE.

Le 16 avril 2009, le contrôleur et le contrôleur adjoint ont présenté un résumé du rapport annuel 2008 du CEPD à la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen.

Brochure d'information

Dans le cadre du deuxième mandat du CEPD (2009-2014), une nouvelle brochure d'information a été développée en 2009. Elle vise le public au sens large et fournit des informations sur les compétences et les missions du CEPD, les droits des personnes concernées, le rôle des délégués à la protection des données et la procédure de dépôt d'une réclamation auprès du CEPD. Elle contient également des lignes directrices et de brèves explications sur les éléments clés du rôle du CEPD et la protection des données à caractère personnel dans l'administration de l'UE.

Des fiches thématiques sur des questions spécifiques de protection des données seront élaborées en 2010 pour fournir des orientations ciblées au public général et aux parties intéressées.

5.8. Actions de sensibilisation

Participer à des événements promotionnels 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 de l'UE 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 et organes européens ont célébré le 28 janvier 2009 la troisième Journée de la protection des données. Cette date marque l'anniversaire de l'adoption, en 1981, de la convention du Conseil de l'Europe pour la protection des données à caractère personnel (convention 108), le premier instrument international juridiquement contraignant dans le domaine de la protection des données.

Cette manifestation a été l'occasion pour le CEPD de souligner l'importance de la vie privée et de la protection des données, et en particulier de sensibiliser le personnel de l'UE à ses droits et obligations en la matière. Un stand d'information a été présenté trois jours consécutifs dans les bâtiments du Parlement européen, de la Commission européenne et du Conseil. 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 créé en coopération avec les délégués à la protection des données des institutions concernées, qui présentaient également leurs activités. Diverses publications détaillant le rôle du CEPD et son travail ont été distribuées et les visiteurs ont également eu la possibilité de tester leur connaissance des questions liées à la protection des données dans un bref quiz.

Pour la prochaine édition de la Journée de la protection des données, l'objectif sera de renforcer cette action, en particulier grâce à l'utilisation de supports vidéo, et de diversifier les actions dans ce contexte de manière à mieux atteindre les membres du personnel de l'UE et les autres parties concernées.

Journée portes ouvertes de l'UE

Le 9 mai 2009, le bureau du CEPD a participé, comme chaque année, 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. Comme lors de la Journée de la protection des données, différents supports ont été distribués aux visiteurs, ainsi qu'un quiz sur la protection de la vie privée et des données à caractère personnel.

Stand du CEPD à la Commission européenne lors de la journée de la protection des données.

6

ADMINISTRATION, BUDGET ET PERSONNEL

6.1. Introduction

Le premier mandat des deux contrôleurs a pris fin en janvier 2009. Après les élections de 2008, une nouvelle équipe a été nommée par le Conseil et le Parlement européen pour un mandat de cinq ans.

Pour bénéficier d'une réserve de personnel hautement spécialisé, le CEPD a lancé un concours général en matière de protection des données, organisé par l'Office européen de sélection du personnel. La liste de réserve sera disponible à l'été 2010.

L'environnement administratif se développe progressivement en fonction des priorités annuelles, en tenant compte des besoins et de la taille de l'institution.

Le CEPD a adopté de nouvelles règles internes nécessaires au bon fonctionnement de l'institution.

La collaboration avec les autres institutions — Parlement européen, Conseil et Commission européenne — s'est encore renforcée, permettant de faire des économies d'échelle considérables.

6.2. Budget

Le budget adopté par l'autorité budgétaire pour l'exercice 2009 s'élevait à 6 663 026 euros, ce qui représente une augmentation par rapport à 2008, due principalement aux postes supplémentaires, au changement des contrôleurs et à l'espace nécessaire plus important en raison de la croissance de l'institution.

En plus des rémunérations et des dépenses liées aux bâtiments, une grande partie du budget est consacrée aux traductions. Les avis du CEPD sur les propositions législatives sont traduits dans les 23 langues officielles de l'UE et publiés au Journal officiel de l'Union européenne. Les avis sur les contrôles préalables et les autres documents publiés sont également traduits dans les langues de travail du CEPD.

Dans son rapport sur l'exercice financier 2008, la Cour des comptes européenne a affirmé que l'audit n'avait donné lieu à aucune observation.

La Commission européenne a continué de fournir une assistance, en particulier en ce qui concerne les services comptables, le comptable de la Commission ayant également été désigné comptable du CEPD. Le CEPD applique les règles internes de la Commission relatives à l'exécution du budget, dans la mesure où il n'existe pas de règles spécifiques à l'institution.

6.3. Ressources humaines

Le CEPD bénéficie de l'aide effective des services de la Commission en ce qui concerne les tâches liées à la gestion du personnel de l'institution

6.3.1. Recrutement

La visibilité croissante de l'institution se traduit par une augmentation de la charge de travail et par un accroissement de ses tâches. L'augmentation sensible de la charge de travail en 2009 a été décrite dans les chapitres précédents et les ressources humaines ont un rôle fondamental à jouer dans ce contexte. Toutefois, le CEPD a décidé de limiter son taux d'accroissement par une progression contrôlée, afin d'assurer la pleine intégration dans l'organisation et une formation satisfaisante des nouveaux membres.

Le CEPD a accès aux services proposés par l'Office européen de sélection du personnel et participe aux travaux de son conseil d'administration, pour le moment en tant qu'observateur. Il a lancé, en coopération avec l'EPSO, un concours général en matière de protection des données pour recruter du personnel hautement spécialisé. La liste de réserve sera disponible à l'été 2010.

En ce qui concerne le logiciel de gestion des ressources humaines (en particulier pour les missions, les congés et les formations), la Commission a suspendu son ancien projet de logiciel en la matière et a créé Sysper2, qui sera opérationnel pour le CEPD d'ici à la fin 2010.

6.3.2. Programme de stages

Un programme de stages a été créé en 2005. Son 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 quotidiennes du CEPD. Celui-ci 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.

Outre le programme principal 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 stricts d'admission.

Tous les stagiaires, rémunérés ou non, ont contribué à la fois au travail théorique et pratique, tout en acquérant une expérience directe utile.

Sur la base d'accords de niveau de service conclus en 2005 et 2008, le CEPD a bénéficié d'une assistance administrative de la part du bureau des stages de la direction générale de l'éducation et de la culture de la Commission, qui a continué d'apporter un soutien précieux grâce à l'expérience de son personnel.

6.3.3. Programme pour les experts nationaux détachés

Le programme destiné aux experts nationaux détachés (END) a été mis en œuvre en janvier 2006. En moyenne, deux experts nationaux des autorités de protection des données de divers États membres ont été détachés chaque année. Les détachements d'experts nationaux ont permis au CEPD de bénéficier de leurs compétences et de leur expérience professionnelle et d'accroître sa visibilité au niveau national. Dans le même temps, ce programme permet aux END de se familiariser avec les questions de protection des données dans le cadre de l'UE.

Afin de recruter des experts nationaux, le CEPD s'adresse directement aux autorités nationales de 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.

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 autres membres du personnel, comprenant une petite équipe de coordinateurs chargés des aspects opérationnels, sont organisés en deux domaines: supervision et consultation. Un attaché de presse coordonne une petite équipe chargée de l'information. Tous travaillent sous l'autorité directe du contrôleur, du contrôleur adjoint et d'un directeur, responsable du secrétariat.

Cette dernière fonction a été créée à la fin de l'année 2009 et constitue une première étape de la

restructuration de l'organisation qui devrait avoir lieu courant 2010.

6.3.5. Formation

En 2009, l'objectif de la politique de formation interne d'élargir et améliorer les connaissances et les compétences 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, a été poursuivi.

Le personnel du CEPD a accès aux formations organisées au niveau interinstitutionnel. En outre, certains membres ont participé à des formations professionnelles externes pour atteindre l'excellence dans le domaine de la protection des données.

Le plan de formation pour 2009, incluant les besoins en personnel déterminés grâce à une enquête, se basait sur les principaux domaines d'apprentissage définis dans les lignes directrices générales annexées à la décision interne en matière de formation.

Les cours de langue ont représenté une grande partie du nombre total de jours consacrés à la formation en 2009. Le taux de participation élevé confirme le principe que l'apprentissage des langues au CEPD doit principalement servir à améliorer l'efficacité professionnelle et les besoins en matière d'emploi y compris, bien sûr, l'intégration harmonieuse des nouveaux membres du personnel dans l'organisation.

Le CEPD a continué à participer aux travaux des comités interinstitutionnels (groupe de travail interinstitutionnel de l'EEA, groupe interinstitutionnel d'évaluation de la formation de l'EEA, comité interinstitutionnel de la formation linguistique, etc.) dans le but de partager une approche commune dans un secteur où les besoins sont, pour l'essentiel, similaires entre les institutions et de réaliser des économies d'échelle.

En 2009, le CEPD a signé, avec les autres institutions, le protocole sur l'harmonisation des coûts des cours de langue interinstitutionnels et le nouveau protocole de répartition des coûts par institution des projets pédagogiques linguistiques interinstitutionnels.

Un accord de niveau de service a également été signé avec l'EEA autorisant le personnel du CEPD sélectionné pour la certification à participer au programme de formation obligatoire pour la procédure de certification.

6.3.6. Activités sociales

Les nouveaux arrivants sont accueillis personnellement par le contrôleur et le contrôleur adjoint. Outre leur mentor, ils rencontrent aussi les membres de l'unité administrative, qui leur communiquent des informations sur les procédures spécifiques de l'institution et leur remettent le guide administratif du CEPD. Celui-ci a signé 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.) et en leur offrant la possibilité de participer à diverses activités sociales et de réseautage.

Le CEPD participe, en qualité d'observateur, aux réunions du comité consultatif du Parlement européen pour la prévention et la protection au travail, dont l'objectif est d'améliorer l'environnement professionnel. Une réflexion a été lancée sur le bien-être au travail.

Le dialogue social au sein du CEPD a malheureusement dû être interrompu temporairement en raison de la démission et du non-renouvellement du comité du personnel. Une activité sociale en dehors de l'institution pourrait toutefois être organisée.

Le CEPD a continué de développer la coopération interinstitutionnelle en ce qui concerne les gardes d'enfants: les enfants du personnel du CEPD ont ainsi accès aux crèches, aux garderies et aux centres extérieurs réservés aux enfants du personnel de la Commission, ainsi qu'aux écoles européennes.

6.4. Fonctions de contrôle

6.4.1. Contrôle interne

Le système de contrôle interne, en vigueur depuis 2006, garantit que les objectifs du CEPD seront réalisés de manière efficace dans le respect des règles. Le CEPD a adopté des procédures de contrôle interne spécifiques en fonction de ses besoins, de sa taille et de ses activités. Le système a été conçu pour gérer plutôt que d'éliminer le risque de non-réalisation des objectifs de l'organisation.

En 2009, l'évaluation des risques liés aux activités du CEPD s'est poursuivie dans le but de concevoir un système de gestion des risques permettant de déterminer et d'évaluer les risques liés à ses activités et, si nécessaire, de prendre des mesures pour les contrer.

Le CEPD a pris acte du rapport d'activité annuel 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 quant à la légalité et la régularité des opérations dont l'institution est responsable.

6.4.2. Audit interne

L'auditeur interne de la Commission a été nommé auditeur interne du CEPD.

Pour garantir la gestion efficace des ressources du CEPD, l'auditeur interne procède à des vérifications régulières des systèmes de contrôle interne de l'institution, ainsi que de ses opérations financières.

Un rapport sur l'audit de suivi réalisé en décembre 2008 par le service d'audit interne a été transmis et adopté courant 2009. Ce rapport a confirmé que le système de contrôle interne du CEPD était capable de fournir une assurance raisonnable quant à la réalisation des objectifs de l'institution, même s'il a également décelé certains aspects à améliorer. Pour certains de ceux-ci, des mesures ont déjà été prises, tandis que d'autres seront progressivement mises en place, en fonction de l'évolution des tâches confiées au CEPD.

6.4.3. Sécurité

À la fin de 2008, le CEPD a adopté une décision sur les mesures applicables en matière de sécurité dans l'institution. Cette décision comprend des mesures concernant la gestion des informations confidentielles et de la sécurité informatique, ainsi que les conditions de santé et de sécurité des personnes et des lieux. Une séance d'information a été organisée en 2009 pour promouvoir la sensibilisation à la sécurité et garantir que le personnel est au courant des mesures de sécurité en place.

6.4.4. Délégué à la protection des données

La mise en œuvre interne des dispositions du règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données s'est poursuivie en 2009.

Les notifications au délégué à la protection des données des opérations de traitement de données à caractère personnel identifiées dans l'inventaire du CEPD se sont également poursuivies en 2009. Pour les dossiers soumis à des notifications en vue d'un contrôle préalable, une procédure simplifiée a été prévue, qui tient compte de la position spécifique du CEPD. Un registre des notifications a été créé.

La participation aux réunions du réseau des DPD permet aux DPD du CEPD de partager des expériences et de discuter des questions d'intérêt commun.

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 en outre dans les domaines des technologies de l'information et de l'infrastructure.

Le CEPD a continué de 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, accord qui a été 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 2009, 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, l'équipement des locaux, la sécurité des bâtiments, les travaux d'impression, le courrier, la téléphonie, les fournitures, etc.) et le Conseil (pour ce qui est des traductions).

Un accord de niveau de service a été signé avec l'Office des paiements, couvrant plusieurs activités, notamment la détermination, le calcul et le paiement des droits individuels du personnel actuel et ancien, ainsi que le remboursement des frais de mission, des soins de santé et des expertises.

Sur la base d'une évaluation positive, une prorogation de deux ans a été prévue (de janvier 2010 à janvier 2012). L'accord avec le Conseil européen pour les services de traduction est arrivé à échéance en janvier 2010. Un nouvel accord a été signé avec le Centre de traduction des organes de l'Union européenne, qui se chargera des traductions à partir de 2010.

Les accords de niveau de service existants sont régulièrement mis à jour. En novembre 2009, le CEPD a signé un nouvel accord de niveau de service avec l'école d'administration européenne concernant le programme de formation du personnel à la procédure de certification.

L'accès direct des locaux du CEPD à certaines applications de gestion financière de la Commission a facilité la coopération et l'échange d'informations entre les services de la Commission et le CEPD.

La coopération en cours avec le Parlement européen a garanti la maintenance du site internet du CEPD et a permis d'ajouter une nouvelle fonctionnalité.

Le CEPD a continué à participer aux appels d'offres interinstitutionnels, accroissant ainsi son efficacité dans de nombreux domaines administratifs et évoluant vers plus d'autonomie.

Le CEPD est membre de plusieurs comités interinstitutionnels et groupes de travail, notamment le comité de gestion assurances maladies (CGAM), le comité de préparation pour les questions statutaires (CPQS), le comité du statut, le groupe de travail interinstitutionnel de l'EEA, le groupe interinstitutionnel d'évaluation de la formation et le comité interinstitutionnel pour la formation linguistique. Cette participation a contribué à accroître la visibilité du CEPD auprès des autres institutions et a encouragé l'échange 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. De nouvelles dispositions générales d'application du statut ont également été adoptées.

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.

Un nouveau guide des missions, basé sur celui de la Commission, a été adopté.

Trois décisions internes ont été adoptées en 2009, concernant la période de stage en cas de congé parental ou familial, concernant le congé spécial d'allaitement et le congé spécial en cas de maladie grave d'un enfant.

Le CEPD est une institution relativement nouvelle qui connaît une évolution rapide. En conséquence, les règles et procédures qui sont adaptées aux premières années d'activité pourraient 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

Un nouveau système de gestion du courrier électronique (GEDA) a été mis en œuvre avec succès pour les tâches administratives en janvier 2009, avec l'aide des services du Parlement européen. À l'issue de cette première étape, des études ont été effectuées pour élaborer un système approprié de gestion des documents et des dossiers pour le service de protection des données.

7

PRINCIPAUX OBJECTIFS POUR 2010

Dans le courant de 2009, les premières mesures ont été prises en vue d'une évaluation stratégique des fonctions et missions du CEPD afin de fixer quatre lignes de développement principales pour les quatre prochaines années, ce qui aura des conséquences dans plusieurs domaines, en particulier dans celui de la supervision et de l'organisation interne. Les développements dans les autres domaines seront plus progressifs et suivront les lignes décrites dans le présent rapport annuel.

Les principaux objectifs suivants ont été sélectionnés pour 2010. Les résultats obtenus figureront dans le rapport de l'année prochaine.

- Soutien du réseau des DPD

Le CEPD continuera à apporter un soutien fort aux délégués à la protection des données, en particulier dans les agences créées récemment, et à encourager un échange de compétences et de meilleures pratiques, y compris par l'adoption éventuelle de normes professionnelles, afin de renforcer leur efficacité.

- Rôle du contrôle préalable

Le CEPD mettra un accent accru sur la mise en œuvre des recommandations figurant dans ses avis sur les contrôles préalables et assurera un suivi adéquat. Les opérations de contrôle préalable communes à la plupart des agences continueront de bénéficier d'une attention particulière.

- Lignes directrices horizontales

Le CEPD continuera de développer des lignes directrices sur les questions pertinentes et les rendra disponibles à tous. Des lignes directrices seront publiées concernant la vidéosurveillance, les enquêtes administratives et les procédures disciplinaires, ainsi que sur les modalités d'application concernant les fonctions et missions des délégués à la protection des données.

- Politique d'enquête

Le CEPD publiera une politique globale sur le contrôle du respect et de la mise en œuvre des règles de protection des données dans les institutions et les organes. Celle-ci couvrira tous les moyens appropriés pour mesurer et assurer le respect des règles de protection des données et encouragera la responsabilité institutionnelle pour une bonne gestion des données.

- Portée de la consultation

Le CEPD continuera d'émettre en temps utile des avis et des commentaires sur les propositions de nouvelles législations et de leur garantir un suivi adéquat dans tous les domaines concernés. Une attention particulière sera accordée au plan d'action pour la mise en œuvre du programme de Stockholm.

- Révision du cadre juridique

Le CEPD accordera la priorité au développement d'un cadre juridique global de protection des données couvrant tous les domaines de la politique de l'UE et garantissant une protection efficace en pratique, et il contribuera au débat public lorsque cela se révélera nécessaire et approprié.

- Agenda numérique

Le CEPD accordera une attention particulière à l'agenda numérique de la Commission dans tous les domaines qui ont un impact évident sur la protection des données. Le principe de *Privacy by Design* et sa mise en œuvre pratique seront fortement promus.

- Activités d'information

Le CEPD améliorera ses outils d'information en ligne (site internet et newsletter électronique) pour mieux répondre aux demandes des visiteurs. De nouvelles publications (fiches techniques) seront élaborées concernant des questions thématiques.

- Organisation interne

Le CEPD révisera la structure organisationnelle de son secrétariat afin de garantir une exécution plus efficace et efficiente de ses différentes tâches et missions. Les lignes principales de la nouvelle structure seront publiées sur le site internet.

- Gestion des ressources

Le CEPD continuera de développer ses activités relatives aux ressources financières et humaines et d'améliorer les autres processus de travail internes. Une attention particulière sera accordée à la nécessité d'un espace de bureaux supplémentaire et du développement d'un système de gestion des dossiers.

Annexe A — Cadre juridique

L'article 286 du traité CE, adopté en 1997 dans le cadre du traité d'Amsterdam, prévoit 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 aussi applicables aux institutions et organes communautaires et qu'une autorité de contrôle indépendante doit être instituée.

Les actes communautaires visés dans cette disposition sont la directive 95/46/CE, qui définit le cadre général du droit de la 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 (voir ci-dessous).

En vertu de l'article 286 TCE, le Contrôleur européen de la protection des données a été créé par 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, entré en vigueur en 2001 ([22]). Ce règlement a également décrit les règles appropriées pour les institutions et les organes conformément aux deux directives.

Depuis l'entrée en vigueur du traité de Lisbonne, l'article 286 susmentionné a été remplacé par l'article 16 du traité sur le fonctionnement de l'Union européenne, qui souligne l'importance de la protection des données de manière plus générale. L'article 16 TFUE et l'article 8 de la charte des droits fondamentaux de l'UE — désormais contraignante — prévoient que le respect des règles en matière de protection des données soit soumis à un contrôle exercé par une autorité indépendante.

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 libertés et droits fondamentaux, qui peuvent être affectés par le traitement des données à caractère personnel dans une société moderne. Cette convention, également appelée «Convention 108», a 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, leur permettant ainsi de participer à la libre circulation des données à caractère personnel, soumises à des règles de protection équivalentes. Mais jusqu'à l'adoption de l'article 286 TCE, il n'existait pas de base juridique pour un tel instrument.

Le traité de Lisbonne, entré en vigueur le 1er décembre 2009, 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, qui est devenue juridiquement contraignante autant pour les institutions et organes, que pour les États membres de l'UE lorsqu'ils appliquent le droit de l'Union. 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 relever 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

([22]) JO L 8 du 12.1.2001, p. 1.

mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire». Depuis l'entrée en vigueur du traité de Lisbonne, cela signifie que les institutions et organes de l'UE, autrefois appelés «institutions et organes communautaires», sont soumis au pouvoir et missions de contrôle du CEPD. Il est difficile de dire si le règlement a une portée plus large et couvre des domaines de l'ancien «troisième pilier».

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 l'usage compatible, les catégories particulières de 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 la mise en œuvre au niveau européen de l'ancienne 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. Ces délégués sont chargés d'assurer, d'une manière indépendante, l'application interne des dispositions du règlement, y compris la bonne notification 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 de travail très important et fort apprécié, qu'il convient de développer encore (voir le point 2.2).

Tâches et compétences du CEPD

Les tâches et les pouvoirs du Contrôleur européen de la protection des données sont clairement énoncés aux articles 41, 46 et 47 du règlement (voir annexe B), à la fois en termes généraux et en termes 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. L'article 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 pouvoirs.

Cette présentation des attributions, fonctions et pouvoirs suit, pour l'essentiel, le même schéma que pour les autorités nationales de contrôle: entendre et examiner les réclamations, effectuer d'autres enquêtes, informer les responsables 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 l'accès aux 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 à propos de nouvelles législations — 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 sur la vie privée et d'envisager d'autres solutions éventuelles, y compris dans l'ancien «troisième pilier» (coopération policière et judiciaire en matière pénale). Surveiller les développements 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 constitue aussi 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 de l'ancien «troisième pilier» a une incidence similaire. En tant que membre du groupe de l'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 de l'ancien «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) i) coopère avec les autorités nationales de contrôle mentionnées à l'article 28 de la directive 95/46/CE des pays auxquels cette directive s'applique dans la mesure nécessaire à l'accomplissement de leurs devoirs respectifs, notamment en échangeant toutes informations utiles, en demandant à une telle autorité ou à un tel organe d'exercer ses pouvoirs ou en répondant à une demande d'une telle autorité ou d'un tel organe,

ii) coopère également avec les organes de contrôle de la protection des données institués en vertu du titre VI du traité sur l'Union européenne en vue notamment d'améliorer la cohérence dans l'application des règles et procédures dont ils sont respectivement chargés d'assurer le respect;

g) participe aux activités du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46/CE;

h) détermine, motive et rend publiques les exceptions, garanties, autorisations et conditions mentionnées à l'article 10, paragraphe 2, point b), 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

7e PC	Septième programme-cadre de recherche
ACAC	Accord commercial anti-contrefaçon
ACC	Autorité de contrôle commune
ACCP	Agence communautaire de contrôle des pêches
APD	Autorité chargée de la protection des données
ARES	Système avancé d'enregistrement
BCE	Banque centrale européenne
BEI	Banque européenne d'investissement
BEUC	Bureau européen des unions de consommateurs
CCR	Centre commun de recherche
CCTV	Télévision en circuit fermé
CdC	Cour des comptes européenne
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
CEPD	Contrôleur européen de la protection des données
CESE	Comité économique et social européen
CIG	Conférence intergouvernementale
CJE	Cour de justice de l'Union européenne
CMT	Centre de médecine du travail
CPD	Coordinateur de la protection des données (à la Commission européenne uniquement)
CSO	Centre de service et d'opération
DG ADMIN	Direction générale du personnel et de l'administration
DG EAC	Direction générale de l'éducation et de la culture
DG EMPL	Direction générale de l'emploi, des affaires sociales et de l'égalité des chances
DG INFSO	Direction générale de la société de l'information et des médias
DG JLS	Direction générale de la justice, de la liberté et de la sécurité
DIGIT	Direction générale de l'informatique
DPD	Délégué à la protection des données
EACEA	Agence exécutive «Éducation, audiovisuel et culture»
EACI	Agence exécutive pour la compétitivité et l'innovation
ECDC	Centre européen de prévention et de contrôle des maladies
ECRIS	Système européen d'information sur les casiers judiciaires
EDW	Banque de données des entreprises
EEA	École européenne d'administration
EEE	Espace économique européen
EFSA	Autorité européenne de sécurité des aliments
EIVP	Étude d'impact sur la protection des données et de la vie privée
EMA	Agence européenne des médicaments
EMPL	Commission de l'emploi et des affaires sociales du Parlement européen

EMSA	Agence européenne pour la sécurité maritime
END	Expert national détaché
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
EPSO	Office européen de sélection du personnel
ETF	Fondation européenne pour la formation
EUMC	Observatoire européen des phénomènes racistes et xénophobes
Eurofound	Fondation européenne pour l'amélioration des conditions de vie et de travail
FIDE	Fichier d'identification des dossiers d'enquêtes douanières
FIDE	Fondation espagnole d'investigations sur le droit et les entreprises
FRA	Agence des droits fondamentaux de l'Union européenne
G29	Groupe de travail de l'article 29
GTPJ	Groupe de travail sur la police et la justice
IAS	Service d'audit interne
IDOC	Office d'investigation et de discipline de la Commission
IMI	Système d'information du marché intérieur
IMI	Initiative Médicaments innovants
IUE	Institut universitaire européen
LCC	Liste de conservation commune
LIBE	Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen
MdA	Mémorandum d'accord
NSA	Agence de sécurité nationale
OCDE	Organisation de coopération et de développement économiques
OCEAP	Organisation de coopération économique Asie-Pacifique
OCVV	Office communautaire des variétés végétales
OEDT	Observatoire européen des drogues et des toxicomanies
OHMI	Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles)
OLAF	Office européen de lutte antifraude
ONG	Organisation non gouvernementale
ONU	Organisation des Nations unies
PMO	Office des paiements de la Commission européenne
PNR	Dossier passager
PPE	Personne politiquement exposée
RDT	Recherche et développement technologique
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
SGC	Secrétariat général du Conseil
s-TESTA	Services télématiques transeuropéens sécurisés entre administrations
STI	Systèmes de transport intelligents

SWIFT	Société de télécommunications interbancaires mondiales
TFUE	Traité sur le fonctionnement de l'Union européenne
TI	Technologies de l'information
TIC	Technologies de l'information et de la communication
TIM	Système de gestion du temps
TFP	Tribunal de la fonction publique
UE	Union européenne
VIH	Virus d'immunodéficience humaine
VIS	Système d'information sur les visas

Annexe D — Liste des délégués à la protection des données

ORGANISATION	NOM	ADRESSE ÉLECTRONIQUE
Parlement européen (PE)	Jonathan STEELE	Data-Protection@europarl.europa.eu
Conseil de l'Union européenne (Consilium)	Pierre VERNHES	Data.Protection@consilium.europa.eu
Commission européenne (CE)	Philippe RENAUDIÈRE	Data-Protection-officer@ec.europa.eu
Cour de justice des Communautés européennes (CURIA)	Marc SCHAUSS	Dataprotectionofficer@curia.europa.eu
Cour des comptes européenne (CdC)	Jan KILB	Data-Protection@eca.europa.eu
Comité économique et social européen (CESE)	Maria ARSENE	Data.Protection@eesc.europa.eu
Comité des régions (CdR)	Petra CANDELLIER	Data.Protection@cor.europa.eu
Banque européenne d'investissement (BEI)	Jean-Philippe MINNAERT	Dataprotectionofficer@eib.org
Médiateur européen	Loïc JULIEN	DPO-euro-ombudsman@ombudsman.europa.eu
Contrôleur européen de la protection des données (CEPD)	Giuseppina LAURITANO	Giuseppina.Lauritano@edps.europa.eu
Banque centrale européenne (BCE)	Frederik MALFRÈRE	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 (CdT)	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 (ETF)	Liia KAARLOP	Liia.Kaarlop@etf.europa.eu
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)	Emmanuel MAURAGE	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)	Cecile MARTEL	Cecile.Martel@emcdda.europa.eu

>>>

ORGANISATION	NOM	ADRESSE ÉLECTRONIQUE
Autorité européenne de sécurité des aliments (EFSA)	Claus RÉUNIS	Dataprotectionofficer@efsa.europa.eu
Agence européenne pour la sécurité maritime (EMSA)	Malgorzata NESTEROWICZ	Malgorzata.Nesterowicz@emsa.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	eacea-data-protection@ec.europa.eu
Agence européenne pour la sécurité et la santé au travail (EU-OSHA)	Terry TAYLOR	Taylor@osha.europa.eu
Agence communautaire de contrôle des pêches (ACCP)	Clara FERNANDEZ/ Rieke ARNDT	cfca-dpo@cfca.europa.eu
Autorité de surveillance du GNSS européen (GSA)	Triinu VOLMER	Triinu.Volmer@gsa.europa.eu
Agence ferroviaire européenne (AFE)	Guido STÄRKLE	Dataprotectionofficer@era.europa.eu
Agence exécutive pour la santé et les consommateurs (EAHC)	Beata HARTWIG	Beata.Hartwig@ec.europa.eu
Centre européen de prévention et de 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 des États membres de l'Union européenne (Frontex)	Sakari VUORENSOLA	Sakari.Vuorensola@frontex.europa.eu
Agence européenne de la sécurité aérienne (AESA)	Francesca PAVESI	Francesca.Pavesi@easa.europa.eu
Agence exécutive pour la compétitivité et l'innovation (EACI)	Elena FIERRO SEDANO	Elena.Fierro-Sedano@ec.europa.eu
Agence exécutive du réseau transeuropéen de transport (TEN-T EA)	Elisa Dalle Molle	Elisa.Dalle-Molle@ec.europa.eu
Agence européenne des produits chimiques (ECHA)	Minna HEIKKILA	Minna.Heikkila@echa.europa.eu
Agence exécutive du Conseil européen de la recherche (ERCEA)	Donatella PIATTO	Donatella.Piatto@ec.europa.eu
Agence exécutive pour la recherche (REA)	Evangelos TSAVALOPOULOS	Evangelos.Tsavalopoulos@ec.europa.eu
Fusion à des fins énergétiques (Entreprise commune pour ITER et le développement de l'énergie de fusion)	Radoslav HANAK	Radoslav.Hanak@f4e.europa.eu

>>>

ORGANISATION	NOM	ADRESSE ÉLECTRONIQUE
Entreprise commune SESAR (SESAR)	Daniella PAVKOVIC	Daniella.PAVKOVIC@sesarju.eu
Entreprise commune Artemis	Anne SALAÜN	Anne.Salaun@artemis-ju.europa.eu
Entreprise commune Clean Sky	Silvia POLIDORI	Silvia.Polidori@cleansky.eu
Initiative Médicaments innovants (IMI)	Estefania RIBEIRO	Estefania.Ribeiro@imi.europa.eu
Entreprise commune Piles à combustible et hydrogène	Nicolas BRAHY	Nicolas.Brahy@fch.europa.eu

Annexe E — Liste des avis rendus à la suite d'un contrôle préalable

Procédures d'évaluation — EMA

Avis du 18 décembre 2009 sur les procédures d'évaluation des performances de l'Agence européenne des médicaments (dossier 2007-421)

Postes individuels — Parlement

Avis du 17 décembre 2009 sur la notification d'un contrôle préalable à propos du dossier «Postes individuels» (dossier 2009-650)

Procédure de notation — Conseil

Avis du 15 décembre 2009 sur la notification d'un contrôle préalable à propos du dossier «Procédure de notation des fonctionnaires du Conseil» (dossier 2009-042)

Sélection d'un directeur pour l'EIGE — Parlement

Avis du 8 décembre 2009 sur une notification en vue d'un contrôle préalable pour la sélection d'un directeur pour l'Institut européen de l'égalité des genres (EIGE) (dossier 2008-785)

Système de gestion de la qualité des données EudraVigilance — EMA

Avis reflété dans une lettre du 7 décembre 2009 sur la notification en vue d'un contrôle préalable pour le système de gestion de la qualité des données EudraVigilance (dossier 2009-740)

Gestion des congés — EFSA

Avis du 1er décembre 2009 sur une notification en vue d'un contrôle préalable concernant la gestion des congés au sein de l'EFSA (dossier 2009-455)

Mobilité interne — BEI

Avis du 18 novembre 2009 sur la notification de contrôle préalable à propos du dossier «Mobilité interne» (dossier 2009-253)

Vérification des pointages Flexitime — Conseil

Avis du 12 novembre 2009 sur la notification de contrôle préalable à propos du dossier «Vérification des pointages Flexitime par rapport aux données sur l'accès physique» (dossier 2009-477)

Enquêtes administratives et procédures disciplinaires — CESE

Avis du 9 novembre 2009 sur la notification de contrôle préalable à propos du dossier «Enquêtes administratives et procédures disciplinaires internes au CESE» (dossier 2008-569)

Évaluation à 360 degrés de l'intelligence émotionnelle par l'école européenne d'administration à la Commission européenne — Commission

Avis du 30 octobre sur une notification en vue d'un contrôle préalable concernant l'évaluation à 360 degrés de l'intelligence émotionnelle par l'école européenne d'administration (dossier 2009-100)

Assurances des députés — Parlement

Avis du 27 octobre 2009 sur la notification de contrôle préalable à propos du dossier «Assurances des députés» (dossier 2009-434)

«e-performance» — BEI

Avis du 19 octobre 2009 sur la notification d'un contrôle préalable à propos du dossier «e-performance» (dossier 2008-379)

Exploitation des listes de réserve — CdC

Avis du 5 octobre 2009 sur la notification d'un contrôle préalable à propos du dossier «Exploitation des listes de réserve et des listes d'aptitude pour le recrutement de fonctionnaires, agents temporaires et contractuels» (dossier 2008-433)

Gestion du Centre polyvalent de l'enfance (CPE) — Commission

Avis du 29 septembre 2009 sur la notification d'un contrôle préalable à propos du dossier «Gestion du Centre polyvalent de l'enfance (CPE) — Garderie et Centre d'études: système d'information Loustic et dossiers médicaux» (Luxembourg) (dossier 2009-089)

Système d'aide à la sécurité — Parlement

Avis du 29 septembre 2009 sur une notification en vue d'un avis préalable concernant le «système d'aide à la sécurité» (dossier 2009-225)

Sélection du personnel permanent et temporaire — Conseil

Avis du 28 septembre 2009 sur la notification de contrôle préalable à propos du dossier «Sélection du personnel permanent et temporaire au secrétariat général du Conseil de l'Union européenne» (dossier 2009-197)

Sélection et recrutement d'agents temporaires et contractuels — FRA

Avis du 24 septembre 2009 sur la notification en vue d'un contrôle préalable concernant la sélection et le recrutement par la FRA de ses agents temporaires et contractuels (dossier 2008-589)

Conseil de discipline — Commission

Avis du 21 septembre 2009 sur la notification d'un contrôle préalable à propos du dossier «Conseil de discipline» (dossier 2009-087)

Assurance accident — Conseil

Avis du 14 septembre 2009 sur la notification d'un contrôle préalable à propos du dossier «Traitement de données dans le cadre de l'assurance accident» (dossier 2009-257)

Base de données EudraVigilance — EMA

Avis du 7 septembre 2009 sur une notification en vue d'un contrôle préalable concernant la base de données EudraVigilance (dossier 2008-402)

Évaluation du président et du vice-président — OCVV

Avis du 28 juillet 2009 sur une notification en vue d'un contrôle préalable concernant l'évaluation du président et du vice-président de l'OCVV (dossiers 2009-355 et 2009-356)

Temps partiel — CdR

Avis du 27 juillet 2009 sur la notification d'un contrôle préalable à propos des demandes d'exercice de l'activité à temps partiel (dossier 2009-396)

Temps partiel — CESE

Avis du 24 juillet 2009 sur la notification d'un contrôle préalable à propos des demandes d'exercice de l'activité à temps partiel (dossier 2009-322)

Recrutement — CdC

Avis du 23 juillet 2009 sur la notification d'un contrôle préalable à propos du dossier «Procédures de sélection pour le recrutement de fonctionnaires, agents temporaires et agents contractuels» (dossier 2008-313)

Auditions des commissaires désignés — Parlement

Avis du 3 juillet 2009 sur la notification de contrôle préalable concernant le traitement de données à caractère personnel lors des auditions de commissaires désignés (dossier 2009-0332)

Évaluation de la formation — BCE

Avis du 1er juillet 2009 sur une notification en vue d'un contrôle préalable concernant l'évaluation de la formation (dossier 2009-220)

Procédures d'appels d'offres — CESE

Avis du 30 juin 2009 sur la notification d'un contrôle préalable sur les procédures d'appels d'offres et de gestion des contrats (dossier 2009-323)

Gestion des présences et des absences — ECDC

Avis du 22 juin 2009 sur la notification de contrôle préalable relative à la «gestion des présences et des absences» (dossier 2009-072)

Sélection du personnel d'encadrement intermédiaire et des conseillers — Commission

Avis du 17 juin 2009 sur une notification de contrôle préalable concernant la sélection du personnel d'encadrement intermédiaire et des conseillers (dossier 2008-751)

Recrutement des agents contractuels — CdR

Avis du 16 juin 2009 sur la notification d'un contrôle préalable à propos du dossier «Recrutement des agents contractuels» (dossier 2008-696)

Recrutement des fonctionnaires — CdR

Avis du 16 juin 2009 sur la notification de contrôle préalable à propos du dossier «Recrutement des fonctionnaires» (dossier 2008-694)

Recrutement des agents temporaires — CdR

Avis du 16 juin 2009 sur la notification de contrôle préalable à propos du dossier «Recrutement des agents temporaires» (dossier 2008-695)

Documents fournis lors du recrutement — Commission

Avis du 5 juin 2009 sur la notification d'un contrôle préalable concernant le dossier «Documents fournis lors du recrutement» (dossier 2008-755)

Déclarations d'intérêt spécifiques — EFSA

Avis du 5 juin 2009 sur une notification en vue d'un contrôle préalable concernant le traitement des déclarations d'intérêt annuelles et spécifiques (dossier 2008-737)

Gestion des stages — Commission

Avis du 5 juin 2009 sur la notification d'un contrôle préalable à propos du dossier «Application de gestion des stages» (dossier 2008-485)

Sécurité du travail au CCR — Commission

Avis du 20 mai 2009 sur une notification de contrôle préalable à propos de la gestion de la sécurité au travail au sein de l'Institut pour la santé et la protection des consommateurs du Centre commun de recherche à Ispra (dossier 2008-541)

Centrale de données d'entreprises — Commission

Avis du 19 mai 2009 sur la notification d'un contrôle préalable à propos du traitement de données à caractère personnel contenues dans la centrale de données d'entreprises de la DG ENTR (dossier 2008-487)

Prévention du harcèlement — Parlement

Avis du 19 mai 2009 sur la notification de contrôle préalable relative à la prévention du harcèlement (dossier 2008-477)

Demandes de stage et recrutement de stagiaires — EMA

Avis du 18 mai 2009 sur la notification d'un contrôle préalable à propos des demandes de stage et du recrutement de stagiaires (dossier 2008-730)

Promotion et reclassement — CdT

Avis du 18 mai 2009 sur la notification d'un contrôle préalable à propos du dossier «Procédure de promotion et de reclassement» (dossier 2009-018)

Service de médiation — Commission

Avis du 18 mai 2009 sur la notification en vue d'un contrôle préalable concernant le service de médiation de la Commission européenne (dossier 2009-010)

TFlow/PROFIL — Parlement

Avis du 8 mai 2009 sur la notification en vue d'un contrôle préalable sur le traitement «TFlow/PROFIL» (dossier 2009-069)

Procédures de recrutement dans certaines agences communautaires

Avis du 7 mai 2009 sur les notifications de contrôle préalable de certaines agences communautaires concernant les procédures de recrutement (dossier 2009-287)

Évaluations et rapports de stage — EFSA

Avis du 6 mai 2009 sur la notification de contrôle préalable concernant les «évaluations et rapports de stage» (dossier 2009-030)

Horaire flexible — CJE

Avis du 6 mai 2009 sur la notification d'un contrôle préalable de la Cour de justice à propos du dossier «Horaire flexible» (dossier 2007-437)

Entretien annuel — ETF

Avis du 4 mai 2009 sur la notification de contrôle préalable concernant l'«entretien annuel ETF» (dossier 2009-168)

Enregistrements sonores au CCR-IE — Commission

Avis du 29 avril 2009 sur une notification en vue d'un contrôle préalable sur les enregistrements sonores à l'Institut de l'énergie du Centre commun de recherche (CCR-IE) à Petten (dossier 2008-014)

Données médicales des enfants des crèches interinstitutionnelles — Commission

Avis du 27 avril 2009 sur la notification d'un contrôle préalable à propos du dossier «Gestion des données médicales des enfants accueillis dans les crèches et jardins d'enfants institutionnels gérés par l'OIB» (dossier 2009-088)

Procédure de sélection des experts nationaux détachés — FRA

Avis du 27 avril 2009 sur la notification de contrôle préalable concernant les procédures de sélection des experts nationaux détachés (dossier 2008-747)

Jeunes experts en délégation — Commission

Avis du 22 avril 2009 sur la notification d'un contrôle préalable à propos du dossier «Jeunes experts en délégation» (dossier 2008-754)

Retraite anticipée — CESE

Avis du 1er avril 2009 sur la notification d'un contrôle préalable à propos du dossier «Exercice annuel de retraite anticipée sans réduction des droits à pension» (dossier 2008-719)

Stagiaires structurels — Commission

Avis du 30 mars 2009 sur la notification en vue d'un contrôle préalable concernant les stagiaires structurels (dossier 2008-760)

Levée d'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission — Commission

Avis du 25 mars 2009 sur la notification d'un contrôle préalable à propos du dossier «traitement des demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission» (dossier 2008-645)

Gestion des informations transmises par l'OLAF — Commission

Avis du 23 mars 2009 sur la notification de contrôle préalable à propos de la gestion des informations transmises par l'OLAF dans le cadre du mémorandum d'accord (dossier 2009-011)

Procédure de fin de stage — Commission

Avis du 10 mars 2009 sur la notification d'un contrôle préalable à propos du dossier «Procédure de fin de stage» (dossier 2008-720)

Flexitime — ETF

Avis du 26 février 2009 sur une notification en vue d'un contrôle préalable relatif à la procédure ETF — Flexitime (dossier 2008-697)

Réintégration et réorientation professionnelle — Conseil

Avis du 23 février 2009 sur la notification d'un contrôle préalable à propos du dossier «Groupe de réintégration et de réorientation professionnelle» (dossier 2008-746)

Agents temporaires — OCVV

Avis du 20 février 2009 sur la notification de contrôle préalable à propos du dossier «Engagement d'agents temporaires et recours à ceux-ci au sein de l'Office communautaire des variétés végétales» (dossier 2008-315)

Retraite anticipée — Parlement

Avis du 18 février 2009 sur la notification d'un contrôle préalable concernant la procédure de retraite anticipée sans réduction des droits à pension (dossier 2008-748)

Outil de vérification et de concordance — CdC

Avis du 9 février 2009 sur une notification en vue d'un contrôle préalable concernant l'outil de vérification et de concordance ART (dossier 2008-239)

Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme — Commission

Avis du 26 janvier 2009 sur la notification de contrôle préalable à propos du dossier «Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme» (dossier 2008-440)

Capacité de travailler dans une troisième langue avant une première promotion — Parlement

Avis du 21 janvier 2009 sur la notification de contrôle préalable sur l'évaluation de la capacité des fonctionnaires de travailler dans une troisième langue avant une première promotion (dossier 2008-690)

Rapports de stage — Parlement

Avis du 21 janvier 2009 sur la notification d'un contrôle préalable concernant les «rapports de stage» (dossier 2008-604)

Commissions d'invalidité — Conseil

Avis du 16 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier «Procédure relative aux commissions d'invalidité» (dossier 2008-626)

Base de données Syslog Formation — Commission

Avis du 16 janvier 2009 sur une notification de contrôle préalable portant sur la gestion de la formation centrale et locale par l'intermédiaire de la base de données Syslog Formation (dossier 2008-481)

Gestion de la crèche — Conseil

Avis du 15 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier «Gestion et facturation de la crèche du secrétariat général du Conseil» (dossier 2007-441)

Retraite anticipée — CdC

Avis du 9 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier «Exercice annuel de retraite anticipée sans réductions des droits à pension» (dossier 2008-552)

Annexe F — Liste des avis sur des propositions législatives

Mesures restrictives à l'encontre de la Somalie e.a.

Avis du 16 décembre 2009 sur différentes propositions législatives instituant certaines mesures restrictives spécifiques à l'encontre de la Somalie, du Zimbabwe, de la Corée du Nord et de la Guinée

Agence pour les systèmes d'information à grande échelle

Avis du 7 décembre 2009 sur la proposition de règlement du Parlement européen et du Conseil portant création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans l'espace de liberté, de sécurité et de justice, et sur la proposition de décision du Conseil confiant à l'agence les tâches relatives à la gestion opérationnelle du SIS II et du VIS en application du titre VI du traité UE

Lutte contre la fraude dans le domaine de la taxe sur la valeur ajoutée

Avis du 30 octobre 2009 sur la proposition de règlement du Conseil concernant la coopération administrative et la lutte contre la fraude dans le domaine de la taxe sur la valeur ajoutée (refonte)

Accès à Eurodac à des fins répressives

Avis du 7 octobre 2009 sur les propositions relatives à l'accès à Eurodac à des fins répressives

Mesures restrictives à l'encontre d'Al-Qaida et des Taliban

Avis du 28 juillet 2009 concernant la proposition de règlement du Conseil modifiant le règlement (CE) n° 881/2002 instituant certaines mesures restrictives spécifiques à l'encontre de certaines personnes et entités liées à Oussama ben Laden, au réseau Al-Qaida et aux Taliban, JO C 276 du 17.11.2009, p. 1

Systèmes de transport intelligents

Avis du 22 juillet 2009 concernant la communication de la Commission sur le plan d'action pour le déploiement de systèmes de transport intelligents en Europe et la proposition de directive du Parlement européen et du Conseil établissant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport

«Programme de Stockholm» — Un espace de liberté, de sécurité et de justice au service des citoyens

Avis du 10 juillet 2009 sur la communication de la Commission intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens», JO C 276 du 17.11.2009, p. 8

Pharmacovigilance

Avis du 22 avril 2009 sur les propositions de règlement et de directive en ce qui concerne la pharmacovigilance, JO C 229 du 23.9.2009, p. 19

Emploi de l'informatique dans le domaine des douanes

Avis du 20 avril 2009 sur l'initiative de la République française en vue de l'adoption d'une décision du Conseil sur l'emploi de l'informatique dans le domaine des douanes, JO C 229 du 23.9.2009, p. 12

Collection d'informations statistiques par la Banque centrale européenne

Avis du 8 avril 2009 sur la recommandation pour un règlement du Conseil modifiant le règlement (CE) n° 2533/98 concernant la collecte d'informations statistiques par la Banque centrale européenne, JO C 192 du 15.8.2009, p. 1

Transplantation d'organes

Avis du 5 mars 2009 sur la proposition de directive relative aux normes de qualité et de sécurité des organes humains destinés à la transplantation, JO C 192 du 15.8.2009, p. 6

Politique commune de la pêche

Avis du 4 mars 2009 sur la proposition de règlement du Conseil instituant un régime communautaire de contrôle afin d'assurer le respect des règles de la politique commune de la pêche, JO C 151 du 3.7.2009, p. 11

Asile: règlement Eurodac

Avis du 18 février 2009 sur la proposition de règlement concernant la création du système «Eurodac»

pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (CE) n° [.../...][établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride] [COM(2008) 825], JO C 229 du 23.9.2009, p. 6

Asile: règlement de Dublin

Avis du 18 février 2009 sur la proposition de règlement établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride [COM(2008) 820 final], JO C 229 du 23.9.2009, p. 1

Niveau minimal de stocks de pétrole brut et de produits pétroliers

Avis du 3 février 2009 sur la proposition de directive faisant obligation aux États membres de maintenir un niveau minimal de stocks de pétrole brut et/ou de produits pétroliers, JO C 128 du 6.6.2009, p. 42

Deuxième avis sur la vie privée et les communications électroniques

Deuxième avis du 9 janvier 2009 relatif au réexamen de 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 128 du 6.6.2009, p. 28

Annexe G — Les discours du contrôleur et du contrôleur adjoint

Tout au long de l'année, le contrôleur et le contrôleur adjoint ont continué de consacrer beaucoup de temps et d'efforts à l'explication de leur 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.

Le contrôleur a fréquemment participé à des réunions de la commission LIBE du Parlement européen ou à des événements connexes. Le 5 mars, il est intervenu lors d'une audition sur les défis liés aux droits fondamentaux sur l'internet. Le 16 avril, il a présenté, avec le contrôleur adjoint, les lignes principales du rapport annuel 2008 du CEPD. Le 27 avril, il s'est exprimé sur la révision en cours du règlement n° 1049/2001 relatif à l'accès du public aux documents. Le 22 juillet, il a présenté son avis sur la communication de la Commission relative au programme de Stockholm. Le 3 septembre, il s'est exprimé lors de la réunion commune des commissions LIBE et ECON sur l'accord intérimaire entre l'UE et les États-Unis sur SWIFT. Le 29 septembre, le contrôleur adjoint s'est exprimé en commission LIBE sur les technologies de l'information à des fins douanières. Le 30 mars, devant la commission ENVI du Parlement européen, il a parlé des questions de protection des données concernant la proposition de directive relative aux transplantations d'organes.

Le contrôleur a également participé à d'autres réunions avec le Parlement européen. Le 22 janvier, il s'est exprimé devant la commission TRAN lors d'une audition sur les systèmes de transport intelligents. Le 28 janvier, il a contribué à la célébration de la Journée de la protection des données au Parlement. Le 10 février, il a présenté son avis sur les droits des patients dans les systèmes de soins de santé transfrontaliers en commission ENVI. Le 29 septembre, il s'est exprimé lors d'une réunion de l'association européenne de la vie privée en coopération avec différents députés du Parlement européen.

Le 26 janvier, le contrôleur a contribué à la célébration de la Journée de la protection des données à la représentation permanente polonaise à Bruxelles. Le 5 mars, il s'est exprimé au Conseil sur la révision du règlement n° 1049/2001 relatif à l'accès du public aux documents. Le 23 mars, il s'est exprimé devant le groupe de travail du Conseil sur la protection des données concernant les priorités en matière de supervision et de consultation. Le 6 juillet, il a fait un discours sur la nécessité d'une stratégie de gestion de l'information à l'échelle de l'UE lors de la première réunion sous la présidence suédoise du groupe de travail du Conseil sur l'échange d'informations. Le 15 juillet, le contrôleur adjoint s'est exprimé au sein du groupe de travail du Conseil concernant l'e-Justice et l'interconnexion des registres d'insolvabilité. Le 7 décembre, le contrôleur a assisté à une audition d'une commission de la chambre des communes sur la protection des données et la répression à la représentation permanente britannique à Bruxelles. Le 28 octobre, le contrôleur adjoint a fait un discours au parlement national de Berlin lors de la célébration des 30 ans de la protection des données et des 10 ans de la liberté de l'information en Allemagne.

Le 26 mars, le contrôleur adjoint s'est exprimé lors d'une audition du Comité économique et social européen sur le déploiement de systèmes de transport intelligents à Ostrava. Le 28 avril, le contrôleur a fait une présentation sur les questions stratégiques liées à la protection des données lors d'une réunion de Riseptis, le comité consultatif de la Commission pour la recherche et l'innovation sur la sécurité, la vie privée et la confiance dans la société de l'information. le 12 mai, il s'est exprimé à une réunion du comité SIS-VIS sur des questions de sécurité des données. Le 14 mai, il a fait un discours à la conférence de la Commission sur l'évaluation de la directive relative à la conservation des données. Le 20 mai, le contrôleur et le contrôleur adjoint se sont tous deux exprimés à la conférence de la Commission sur la protection des données. Le 14 septembre, le contrôleur adjoint est intervenu lors d'une audition au Comité économique et social européen sur les réseaux sociaux à Bruxelles. Le 16 septembre, le contrôleur s'est exprimé lors d'une conférence organisée par l'Agence européenne chargée de la sécurité des réseaux et de l'information à Héraklion. Le 30 septembre, le contrôleur adjoint a participé à l'atelier du CEPD sur la vidéosurveillance au sein des institutions et organes de l'Union. Le 13 mai, il s'est exprimé sur la protection des données au sein des institutions et organes de l'UE lors de la 12e réunion du réseau juridique interagences [Inter Agency Legal Network (IALN)], organisée par l'Office de l'harmonisation dans le marché intérieur (marques, dessins et modèles) (OHMI) à Alicante. Le 4 avril, il s'est exprimé lors d'une conférence internationale sur la liberté de l'information et la protection des données à Viareggio. Le 23 octobre, le contrôleur et le contrôleur

adjoint ont tous deux contribué à un séminaire sur les violations des données organisé par le CEPD en coopération avec l'ENISA.

Le 16 janvier, le contrôleur s'est exprimé sur la protection des données dans le cadre de Schengen et Dublin à l'université de Fribourg, en Suisse. Le 17 janvier, il est intervenu lors de la conférence annuelle sur l'informatique, la vie privée et la protection des données à Bruxelles. Le 27 janvier, il a contribué à une conférence sur la protection des données et la répression à l'institut Clingendael à La Haye. Le 11 février, il a parlé des défis actuels en matière de protection des données au niveau européen lors d'une conférence de la TEPSA (Trans European Policy Studies Association) à Bruxelles. Le 19 février, il a fait une présentation à la conférence e-santé 2009 à Prague. Le 27 février, il s'est adressé à un comité consultatif sur les questions d'e-gouvernement à La Haye. Le 19 mars, il a contribué à une conférence du PSE sur l'internet à Athènes. Le 26 mars, il est intervenu lors d'une conférence de la British Bankers' Association à Londres. Le 3 novembre, le contrôleur adjoint s'est exprimé sur les récents développements en matière de protection des données au niveau européen lors d'un atelier de la FIDE (Fondation espagnole d'investigations sur le droit et les entreprises) à Madrid. Le 14 décembre, il a fait un discours à l'université de Florence sur la protection des données et les codes de conduite et le 17 avril, il s'est exprimé sur la surveillance électronique sur le lieu de travail à l'école supérieure Alma de Bologne.

Le 28 avril, le contrôleur adjoint a fait un discours sur la vie privée et la sécurité au Centre d'études politiques à Bruxelles. Le 8 mai, le contrôleur a contribué à une conférence sur l'internet des objets à Bruxelles. Le 18 mai, il s'est exprimé lors d'une conférence sur la protection des données au niveau de l'UE à Bruxelles. Le 21 mai, il a fait un discours lors de la conférence de printemps de la commission autrichienne des juristes à Weissenbach am Attersee. Le 8 juin, il est intervenu lors de la 11e conférence sur la protection des données et la sécurité des données à Berlin. Le 19 juin, le contrôleur adjoint s'est exprimé lors d'une conférence des magistratures européennes sur la surveillance et la protection des droits fondamentaux à Vienne. Le 23 juin (vie privée et sécurité au niveau mondial) et le 10 septembre (affaires liées à la protection des données portées devant les tribunaux européens), il s'est exprimé lors de deux conférences du conseil supérieur de la justice italien destinées aux juges et aux procureurs.

Le 8 septembre, le contrôleur a prononcé un discours lors du séminaire intitulé «Transparence et clarté du langage juridique dans l'UE» organisé par la présidence suédoise à Stockholm. Le 21 septembre, il s'est exprimé lors d'une conférence sur le gouvernement et l'informatique à Anvers. Le 24 septembre, il s'est rendu à l'autorité slovaque de protection des données à Bratislava. Le 8 octobre, il est intervenu lors du 35e anniversaire de la section néerlandaise de la Commission internationale des juristes (NJCM) à La Haye. Les 8 et 9 octobre, le contrôleur et le contrôleur adjoint ont contribué à un atelier sur la protection des données dans les procédures pénales à Strasbourg. Le 13 octobre, le contrôleur s'est exprimé lors d'une conférence du groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée à Paris. Le 14 octobre, il a participé à une conférence sur la sécurité et la vie privée à Oslo. Le 26 octobre, il s'est exprimé lors d'un déjeuner-réunion de l'association belgo-néerlandaise (BENEV) à Bruxelles. Le 28 octobre, il s'est exprimé lors d'une conférence de Missing Children Europe à Bruxelles.

Le 2 novembre, le contrôleur s'est exprimé lors d'un atelier sur le concept de *Privacy by Design* à Madrid. Le 3 novembre, il est intervenu lors d'une conférence de la société civile à Madrid. Le 12 novembre, il s'est exprimé lors d'un séminaire sur le programme de Stockholm organisé par la Fondation Robert Schuman à Bruxelles ainsi que lors d'une conférence du Bureau européen des unions de consommateurs (BEUC) sur la vie privée des consommateurs à Bruxelles. Le 20 novembre, il a fait un discours lors d'une conférence nationale néerlandaise sur la vie privée à Amsterdam. Le 2 décembre, il est intervenu sur les questions d'e-santé lors d'une conférence organisée par les amis de l'Europe à Bruxelles. Le 3 décembre, il s'est exprimé sur les systèmes de transport intelligents lors de la 9e conférence des commissionnaires de transport à Bruxelles.

Le contrôleur et le contrôleur adjoint ont également été impliqués dans les relations transatlantiques. Le 12 mars, le contrôleur a fait une présentation lors du sommet sur la vie privée de l'IAPP à Washington DC. Le 26 mai, le contrôleur adjoint a fait un discours lors du premier séminaire Europe-Amérique latine sur la protection des données à Cartagena de Indias, en Colombie. Du 16 au 18 novembre, le contrôleur et le contrôleur adjoint ont contribué à la conférence sur la sphère de sécurité organisée par le département américain du commerce à Washington DC.

Annexe H — Composition du secrétariat du CEPD

Monique LEENS-FERRANDO
Chef du secrétariat (depuis novembre 2009)

• Supervision

Sophie LOUVEAUX *Administrateur/Conseiller juridique* *Coordinatrice pour les relations avec les DPD et les contrôles préalables*	Manuel GARCIA SANCHEZ *Expert national/Conseiller Technologies* *(jusqu'en octobre 2009)*
	Delphine HAROU *Assistante Supervision*
Zsuzsanna BELENYESSY *Administrateur/Conseiller juridique*	John-Pierre LAMB *Expert national (depuis octobre 2009)*
Isabelle CHATELIER *Administrateur/Conseiller juridique*	Xanthi KAPSOSIDERI *Assistante Supervision*
Eva DIMOVNÉ KERESZTES *Administrateur/Conseiller juridique* *Coordinatrice pour les contrôles* *(jusqu'en octobre 2009)*	Sylvie PICARD *Assistante Supervision*
Jaroslaw LOTARSKI *Administrateur/Conseiller juridique* *Coordinateur pour les réclamations*	Kim Thien LÊ *Assistante Secrétariat*
Maria Veronica PEREZ ASINARI *Administrateur/Conseiller juridique* *Coordinatrice pour les mesures administratives*	Pierre FALLER *Stagiaire (avril 2009 à juillet 2009)*
Tereza STRUNCOVA *Administrateur/Conseiller juridique*	Evangelia MESAIKOU *Stagiaire (mars 2009 à juillet 2009)*
Michaël VANFLETEREN *Administrateur/Conseiller juridique*	Eleni ATHERINOU *Stagiaire (depuis octobre 2009)*
Athena BOURKA *Expert national/Conseiller Technologies* *(jusqu'en octobre 2009)*	Mathias POCS *Stagiaire (depuis octobre 2009)*

• Politique et information

Hielke HIJMANS *Administrateur/Conseiller juridique* *Coordinateur Consultation et procédures devant la Cour*	Roberto LATTANZI *Expert national (depuis octobre 2009)*
Rosa BARCELO *Administrateur/Conseiller juridique*	Martine BLONDEAU (*) *Assistante Documentation*
Laurent BESLAY *Administrateur/Conseiller Technologies* *Coordinateur Sécurité et technologies*	Francisco Javier MOLEÓN GARCIA *Assistant Documentation*
Katarzyna CUADRAT-GRZYBOWSKA *Administrateur/Conseiller juridique*	Andrea BEACH *Assistante Secrétariat*
Bénédicte HAVELANGE *Administrateur/Conseiller juridique* *Coordinatrice Grands systèmes TI et politique des frontières*	Anna-Maria VANHOYE *Assistante Secrétariat (depuis octobre 2009)*
Herke KRANENBORG *Administrateur/Conseiller juridique*	Vasiliki MYLONA *Stagiaire (mars 2009 à juillet 2009)*
Anne-Christine LACOSTE *Administrateur/Conseiller juridique* *Coordinatrice groupe article 29*	Mario VIOLA DE AZEVEDO CUNHA *Stagiaire (mars 2009 à juillet 2009)*
Alfonso SCIROCCO *Administrateur/Conseiller juridique*	Maria-Grazia PORCEDDA *Stagiaire (depuis octobre 2009)*
Nathalie VANDELLE (*) *Administrateur/Attachée de presse* *Coordinatrice équipe Information*	

(*) Équipe Information.

• Unité Personnel/Budget/Administration

Monique LEENS-FERRANDO
Chef d'unité (jusqu'en octobre 2009)

• Ressources humaines

Giuseppina LAURITANO *Administrateur/Conseiller Questions statutaires et audits/Déléguée à la protection des données*	Guido CAGNONI *Stagiaire (mars 2009 à juillet 2009)*
Vittorio MASTROJENI *Assistant Ressources humaines*	Livia HARSEU *Stagiaire (depuis octobre 2009)*
Anne LEVÊCQUE *Assistante Ressources humaines*	

• Budget et finances

Tonny MATHIEU *Administrateur financier (jusqu'en octobre 2009)*	Maria SANCHEZ LOPEZ *Assistante Questions financières et comptabilité*
Raja ROY *Assistant Questions financières et comptabilité*	

• Administration

Anne-Françoise REYNDERS *Activités sociales, Infrastructures, Assistante administrative*

Le CEPD, le Contrôleur adjoint et leurs collaborateurs.

Le Contrôleur européen de la protection des données

Rapport annuel 2009

Luxembourg: Office des publications de l'Union européenne

2011 — 114 p. — 21 x 29,7 cm

ISBN 978-92-95073-04-3
doi:10.2804/12053

COMMENT VOUS PROCURER LES PUBLICATIONS DE L'UNION EUROPÉENNE?

Publications gratuites:

- sur le site de l'EU Bookshop (http://bookshop.europa.eu);
- auprès des représentations ou des délégations de l'Union européenne. Vous pouvez obtenir leurs coordonnées en consultant le site http://ec.europa.eu ou par télécopieur au numéro +352 2929-42758.

Publications payantes:

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

Abonnements facturés (par exemple séries annuelles du *Journal officiel de l'Union européenne*, recueils de la jurisprudence de la Cour de justice de l'Union européenne):

- auprès des bureaux de vente de l'Office des publications de l'Union européenne (http://publications.europa.eu/others/agents/index_fr.htm).

QT-AA-10-001-FR-C

CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Le gardien européen de la protection des données personnelles

www.edps.europa.eu

Office des publications

ISBN 978-92-95073-04-3