Avis sur la notification en vue d'un contrôle préalable adressée par le délégué à la protection des données («DPD») de l'Office européen de lutte antifraude («OLAF») le 17 octobre 2007 concernant le système de télévision en circuit fermé (système de CCTV) de l'OLAF

Bruxelles, le 19 mai 2008 (dossier 2007-0634)

1. Procédure

Le 17 octobre 2007, le DPD de l'OLAF a présenté une notification en vue d'un contrôle préalable (la «**notification**») au Contrôleur européen de la protection des données («**CEPD**») à propos du traitement des données prévu par l'OLAF concernant son nouveau système de télévision en circuit fermé.

Le 24 novembre 2007, le CEPD a demandé des informations préliminaires supplémentaires à l'OLAF. Le DPD de l'OLAF a répondu le 26 novembre 2007. Le même jour, le CEPD a sollicité des informations complémentaires. L'OLAF a répondu le 28 novembre 2007. Le même jour, le CEPD a envoyé à l'OLAF une troisième série de questions pour obtenir des informations complémentaires.

Le 7 décembre 2007, l'OLAF a envoyé au CEPD une version actualisée de sa notification. Le même jour, le CEPD a formulé en plus de ses demandes d'informations précédentes et envoyé à l'OLAF une quatrième et dernière série de questions. L'OLAF a répondu aux questions restantes du CEPD (troisième et quatrième séries de questions) le 13 mars 2008.

Le 3 avril 2008, le CEPD a envoyé au DPD de l'OLAF un résumé expliquant la manière dont il comprenait les faits, afin de s'assurer de l'exactitude des informations reçues de l'OLAF. Jusqu'à ce que l'OLAF ait envoyé par écrit une confirmation finale des faits, le 17 avril 2008, le dossier est resté en suspens.

Enfin, la procédure a été suspendue pendant 29 jours, entre le 17 avril 2008 et le 16 mai 2008, période durant laquelle l'OLAF a rédigé ses commentaires sur le projet d'avis du CEPD.

2. Faits

2.1. Champ d'application de la notification. Le bâtiment de la Commission où se trouve l'OLAF est équipé de deux systèmes de télévision en circuit fermé (CCTV):

- le système de CCTV de l'OLAF, qui ne couvre que les locaux sécurisés de l'OLAF; et
- celui de la Commission, qui couvre les zones du bâtiment situées hors du périmètre de sécurité de l'OLAF. Ce système est géré par la Direction Sécurité de la Direction générale du personnel et de l'administration de la Commission («**Direction Sécurité**»

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
E-mail : edps@edps.europa.eu - Site Web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

et «**DG ADMIN**»). Il concerne un périmètre différent et plus vaste que celui du système de CCTV de l'OLAF.

De ces deux systèmes, seul celui installé et commandé par l'OLAF est concerné par la notification et relève du champ d'application du présent avis sur la notification en vue d'un contrôle préalable. Le système de CCTV de l'OLAF a déjà été installé, mais ne sera mis en service que lorsque le CEPD aura publié le présent avis et que l'OLAF aura mis en œuvre les recommandations qui y sont formulées.

2.2. Emplacement et champ de vision des caméras. Le système de CCTV de l'OLAF comprend 49 caméras, toutes situées à l'intérieur du périmètre sécurisé de l'OLAF au sein du bâtiment de la Commission abritant l'OLAF.

Le système de CCTV de l'OLAF couvre tout d'abord les entrées et sorties de ses locaux sécurisés [indication des emplacements précis omise dans la version de l'avis disponible sur le site web du CEPD]. Les caméras surveillent les endroits où l'on peut entrer et sortir des locaux, par exemple, à proximité des ascenseurs et à la sortie des escaliers, ainsi qu'à proximité des sorties de secours et des entrées depuis le toit du bâtiment.

En outre, le système surveille, dans une certaine mesure, les zones sensibles où une sécurité physique supplémentaire est requise, notamment:

- le centre de gestion documentaire de l'OLAF, qui contient des documents opérationnels sensibles [indication des emplacements précis omise],
- les salles informatiques [indication des emplacements précis omise],
- la zone de stockage informatique [indication des emplacements précis omise], et
- les salles techniques informatiques [indication des emplacements précis omise], où les connexions des utilisateurs finals au réseau commun de la CE ou au réseau sécurisé de l'OLAF sont matériellement effectuées et où des interventions régulières du personnel de l'OLAF et de la DIGIT sont nécessaires.

En pratique, cela signifie qu'il y a des caméras à chaque étage occupé par l'OLAF. Les salles informatiques, la zone de stockage informatique et les salles techniques informatiques ne sont normalement pas surveillées et contiennent des équipements informatiques très sensibles, ainsi que des équipements informatiques communs de la Commission. L'OLAF souhaite pouvoir vérifier quel équipement a fait l'objet d'une intervention technique dans ces salles. Ce point est particulièrement important, dans la mesure où des interventions de personnel externe peuvent occasionnellement être nécessaires dans ces locaux.

Aucune caméra ne surveille des zones où du personnel serait présent en permanence et il n'existe aucun cas où un membre du personnel travaillant dans une certaine zone serait constamment dans le champ de vision d'une caméra.

Il n'y a pas non plus de caméra dans les bureaux individuels, dans les cafétérias/cuisines, à proximité des toilettes ou à l'intérieur, ni dans d'autres endroits où les membres du personnel et les visiteurs attendent un degré élevé d'intimité.

Le champ de vision des caméras n'est pas non plus dirigé vers des parties du bâtiment de la Commission occupées par d'autres services que l'OLAF.

Au rez-de-chaussée, des caméras sont installées à proximité de l'accueil, elles ne sont cependant orientées que vers les ascenseurs et les escaliers et ne filment que les personnes

entrant ou quittant l'OLAF. Une personne doit avoir passé les portes de contrôle automatique d'accès avant d'être filmée par le système. Il n'y a pas de caméra dans les escaliers, les ascenseurs ou les couloirs aux étages qui ne donnent pas accès au périmètre sécurisé de l'OLAF.

Les caméras dans le parking sont celles du système de CCTV de la Commission.

Enfin, le champ de vision des caméras n'est pas non plus orienté vers des zones situées hors du bâtiment sur le territoire belge, vers les rues, les bâtiments ou toute autre zone publique ou privée dans les environs.

2.3. Qualité de l'image. La résolution des caméras est de 1280 X 960 pixels. Cela permet à l'OLAF de filmer les visages de manière reconnaissable.

2.4. Détection des mouvements. Toutes les caméras de l'OLAF sont équipées de la fonction de détection des mouvements. Elle sera activée sur toutes les caméras afin de déclencher l'enregistrement vidéo. La détection de mouvement limitera le signal vidéo aux événements justifiant d'être filmés et enregistrés. Cela signifie que les caméras ne filmeront que lorsqu'un mouvement sera détecté. La détection de mouvement sera utilisée en permanence, 24 heures sur 24, 7 jours sur 7, pendant les heures de bureau et en dehors. La caméra ajoute automatiquement l'information de mouvement au flux des données envoyées au dispositif d'enregistrement, qui n'enregistrera que si une caméra l'informe qu'elle a détecté des mouvements.

2.5. Enregistrement du son. Dans son commentaire sur le projet d'avis du CEPD, l'OLAF a fait remarquer au CEPD un nouvel élément concernant les faits du dossier, à savoir que les caméras peuvent enregistrer le son. En effet, l'OLAF a expliqué que la capacité d'enregistrer le son est requise par les termes de référence de l'appel d'offres pour le système de contrôle d'accès «EUCI Registry Visitors» de l'OLAF. La fonction d'enregistrement du son n'a cependant pas encore été activée.

2.6. «Vidéosurveillance haut de gamme», caméras dissimulées à la vue et autres caractéristiques intrusives. L'OLAF ne prévoit pas d'utiliser d'autres techniques ou équipements que l'on peut qualifier de «vidéosurveillance haut de gamme». Par exemple, il ne prévoit pas d'utiliser de système de vidéosurveillance intelligente équipé d'un logiciel de reconnaissance faciale ou d'images, ni d'un logiciel de reconnaissance de la démarche. L'OLAF n'a pas non plus installé de réseau de caméras multiples, pourvu d'un logiciel de suivi capable de suivre les objets ou les personnes se déplaçant dans une zone. Il n'a pas non plus mis en place de caméra dissimulée à la vue (par ex. des caméras dans le toit) ou contrôlées à distance (caméra pan-tilt-zoom). Les caméras ne sont pas non plus équipées de dispositifs d'imagerie thermique lorsqu'il y a peu de lumière (caméras infrarouge ou proche infrarouge).

2.7. Données sensibles. L'OLAF ne prévoit pas d'installer des caméras dans des endroits où il existe une probabilité accrue que des données sensibles (en vertu de l'article 10, paragraphe 1, du règlement (CE) n° 45/2001) soient régulièrement filmées. Cela inclut les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle. Par exemple, l'OLAF n'a pas de caméra dans les zones situées en dehors de ses bâtiments où des manifestants seraient potentiellement dans le champ de vision des caméras, ni à l'entrée du bureau d'un assistant

social, d'un syndicat ou d'un comité du personnel. Il n'y a pas d'endroits destinés à la prestation de services médicaux ou à des fins religieuses dans les locaux sécurisés de l'OLAF.

2.8. Questions relatives à la finalité du traitement et à la proportionnalité

2.8.1. Risques en matière de sécurité dans les zones couvertes par le système de CCTV de l'OLAF. L'OLAF n'a pas de document interne qui énumèrerait, définirait et évaluerait spécifiquement les risques en matière de sécurité que le système prévu de CCTV doit réduire. L'OLAF a cependant confirmé que les types de risques en matière de sécurité que le système de CCTV est conçu pour prévenir concernent principalement l'accès physique non autorisé et comprend:

- l'accès non autorisé aux locaux sécurisés et salles protégées de l'OLAF;
- l'accès non autorisé aux infrastructures informatiques sécurisées de l'OLAF;
- l'accès non autorisé aux informations opérationnelles de l'OLAF;
- le vol de biens ou d'équipements du personnel ou de la CE;
- les menaces pour la sécurité du personnel de l'OLAF travaillant dans le bureau.

2.8.2. Historique des incidents de sécurité survenus à l'OLAF. Le CEPD a demandé à l'OLAF de fournir des statistiques et des exemples d'incidents qui se sont réellement produits dans les locaux de l'OLAF par le passé. Plus particulièrement, le CEPD a demandé les statistiques des cinq dernières années et une copie du registre des incidents de sécurité de l'OLAF.

L'OLAF a répondu au CEPD qu'il ne disposait pas actuellement d'un registre des incidents de sécurité. L'OLAF a expliqué que le faible nombre d'incidents détectés ne semblait pas nécessiter l'établissement d'un registre de ce type. Il convient toutefois de noter que le faible nombre d'incidents détectés (ainsi que le long délai de détection) peut en partie être dû à l'absence de capacité appropriée de l'OLAF en ce qui concerne la détection des incidents. L'OLAF a confirmé qu'avec l'introduction de son nouveau système de sécurité, un registre officiel des incidents sera mis en place et que les incidents seront régulièrement analysés afin d'améliorer et d'adapter le système comme nécessaire.

Étant donné qu'un registre des incidents de sécurité et des statistiques complètes n'étaient pas disponibles, et que l'OLAF a déclaré prévoir de suivre de plus près le système et son efficacité à l'avenir, le CEPD a accepté que l'OLAF ne décrive que quelques exemples caractéristiques des incidents passés et fournisse une estimation de leur fréquence d'occurrence afin d'illustrer les besoins réels en matière de sécurité de l'OLAF.

L'OLAF a décrit au CEPD trois des principaux incidents de sécurité survenus au cours des cinq dernières années. Ces trois cas concernaient l'accès non autorisé aux locaux sécurisés de l'OLAF et potentiellement aux informations opérationnelles de l'OLAF, en dehors des heures de travail par des personnes non identifiées.

2.8.3. Le rôle d'assistance pour l'OLAF du nouveau système de CCTV en vue de dissuader, prévenir et examiner les incidents de sécurité. L'OLAF a expliqué au CEPD qu'il organisait et mettait actuellement en œuvre des mesures de sécurité spécifiques accrues depuis l'adoption de sa politique en matière de sécurité de l'information, comprenant à la fois des mesures de sécurité physique et informatique, qui amélioreront les capacités de détection des incidents de l'OLAF. Le nouveau système de CCTV fait partie de ces efforts. Il sera nettement plus rapide et facile d'identifier les personnes à l'origine d'incidents analogues de sécurité qui pourraient se produire à l'avenir. Le personnel de sécurité de l'OLAF sera en

mesure de détecter ou de confirmer lors d'une enquête si des personnes ont eu un accès non autorisé à des systèmes informatiques sensibles installés dans les locaux et, le cas échéant, de donner leur identité. Il pourra également prévenir plus efficacement les accès non autorisés lors d'un incident de sécurité. Les avantages du nouveau système de CCTV seront principalement dus:

- aux caméras qui seront installées aux points d'accès et aux autres endroits stratégiques (par ex. les salles informatiques); l'OLAF fait remarquer que trois étages supplémentaires du bâtiment [indication des emplacements précis omise] ont été inclus dans les locaux sécurisés de l'OLAF, après que les caméras de l'ancien système de CCTV de la Commission ont été installées; de nouveaux points d'accès ont donc été ajoutés aux locaux sécurisés de l'OLAF [indication des emplacements précis omise]; le nouveau système surveillera ces points et couvrira également les accès situés sur le toit du bâtiment (une mesure de sécurité imposée par le service d'incendie);

- aux autres endroits stratégiques (par ex. les salles informatiques, comme susmentionné) qui seront également surveillés;

- aux enregistrements qui peuvent être utilisés pour enquêter sur les incidents qui se sont déjà produits;

- au nouveau système de CCTV qui peut également prévenir les incidents en déclenchant une alarme automatiquement signalée à la permanence de sécurité de l'OLAF, permettant une réaction immédiate du personnel de sécurité de l'OLAF.

D'autres caractéristiques techniques apporteront des avantages supplémentaires, notamment:

- les trois systèmes de contrôle physique de l'OLAF seront intégrés (cf. section 2.8.4 ci-après). Par exemple, les horloges des trois systèmes de sécurité de l'OLAF seront synchronisées, il sera ainsi possible de trouver la bonne séquence plus facilement et plus rapidement;

- la résolution des nouvelles caméras est nettement supérieure à celle de l'ancien système, ce qui permet d'obtenir des images plus claires et de procéder plus facilement à l'identification;

- les caméras sont orientées de manière à obtenir des séquences vidéo significatives (par exemple, également du visage et non pas seulement du dos d'une personne à une sortie de secours).

2.8.4. La CCTV fait partie d'un ensemble plus large de systèmes de sécurité physique de l'OLAF.

Le système de CCTV sera l'un des trois systèmes de sécurité physique spécifiques à l'OLAF. Les deux autres systèmes sont:

- le système de contrôle d'accès qui régit l'accès aux locaux sécurisés de l'OLAF, ainsi qu'à l'intérieur, et fait l'objet d'une autre notification soumise au CEPD en vue d'un contrôle préalable, et

- le système de détection des intrusions physiques installé dans certains endroits très sensibles, par exemple les salles informatiques et le centre de gestion des documents de l'OLAF.

En outre, les politiques habituelles de la Commission en matière de sécurité s'appliquent en tant que garanties minimales pour la protection du bâtiment de l'OLAF, la sécurité du personnel, la protection contre les incendies et la protection des informations et des autres biens de la Commission. La Direction Sécurité de la DG ADMIN fournit ces garanties.

L'OLAF a souligné qu'un niveau élevé de sécurité ne peut être atteint qu'en associant plusieurs méthodes de sécurité. Du point de vue de l'OLAF, les exemples d'incidents de sécurité survenus dans le passé (cf. section 2.8.2 ci-dessus) montrent les faiblesses en matière de sécurité du système actuel de contrôle d'accès.

L'OLAF estime en particulier que le système de CCTV permettra de reconstituer ce qui s'est réellement produit aux endroits clés du périmètre sécurisé de l'OLAF lors d'un incident de sécurité, notamment en dehors des heures de bureau normales. Cela n'était pas toujours possible dans le cadre des dispositions de sécurité précédentes.

2.9. Enregistrement et surveillance directe. La séquence est enregistrée, mais n'est pas surveillée en direct sans interruption ou systématiquement, par exemple, par les gardes de sécurité dans une salle de contrôle ou à l'accueil du bâtiment.

Les séquences vidéo ne seront visionnées qu'en cas d'incident de sécurité et si cela se révèle nécessaire,

- pour permettre de déterminer ce qui s'est passé (c'est-à-dire que les vidéos sont enregistrées pour une analyse a posteriori),
- ou si une intervention immédiate est nécessaire. Comme susmentionné, il existe un système d'alerte automatique pour attirer l'attention du personnel de sécurité de l'OLAF sur un incident (le responsable local de la sécurité, son adjoint et les responsables de la sécurité de la gestion du réseau) qui pourra instantanément avoir accès aux vidéos en direct de l'OLAF, si nécessaire.

2.10. Période de conservation. Les données enregistrées ne seront pas conservées plus d'un an. Cela signifie que toutes les séquences de CCTV des 49 caméras peuvent être conservées une année complète, même (i) si aucun incident de sécurité n'a été détecté au cours de cette année, ou (ii) si seules les séquences de certaines caméras sont pertinentes pour enquêter sur les accidents de sécurité qui ont réellement eu lieu. Les vidéos sont stockées en ligne pendant cinq mois, puis déchargées et stockées hors ligne pour sept mois au maximum avant d'être détruites. La période maximale totale de conservation de toute séquence vidéo est ainsi de douze mois.

Néanmoins, si une séquence particulière est pertinente pour l'enquête sur un incident de sécurité, elle sera exportée et placée dans le dossier relatif à l'incident, jusqu'à la fin de l'enquête ou de son suivi final disciplinaire ou judiciaire. Elle sera ensuite détruite.

Aucune donnée n'est conservée à des fins historiques, statistiques ou scientifiques.

Du point de vue de l'OLAF, la période de conservation indiquée est nécessaire, car tous les incidents de sécurité ne sont pas découverts immédiatement. Par exemple, certaines enquêtes de sécurité n'ont été ouvertes que deux ou trois ans après la divulgation d'un document

opérationnel sensible de l'OLAF. De plus, l'OLAF soutient qu'une période totale de conservation d'un an est raisonnable dans son cas, compte tenu de la nature sensible de ses activités opérationnelles.

L'OLAF n'a pas communiqué d'autres données concernant (i) la fréquence de la découverte d'un incident de sécurité dans un délai aussi long et (ii) la raison pour laquelle d'autres mesures techniques et organisationnelles ne peuvent être prises afin de détecter plus tôt les incidents de sécurité enregistrés par le système de CCTV (principalement des accès physiques non autorisés) et, ainsi, d'ouvrir une enquête plus tôt.

2.11. Destinataires

2.11.1 Personnel de sécurité de l'OLAF. Le système de CCTV est utilisé et géré par le personnel de sécurité interne de l'OLAF, composé:

- du responsable local de la sécurité[1],
- du responsable adjoint de la sécurité, et
- de trois agents statutaires responsables de la gestion quotidienne des systèmes de sécurité spécifiques à l'OLAF.

Le chef de l'unité «Services de l'information» de l'OLAF, dont la sécurité fait partie, n'a pas d'accès direct aux séquences des caméras (ni mot de passe, ni moniteur dans son bureau). Il aura cependant un accès indirect grâce à l'un des cinq agents de sécurité de l'OLAF, si cela se révèle nécessaire, par exemple lorsqu'une décision doit être prise sur le transfert de certaines séquences de CCTV à un tiers. Dans ce cas notamment où des questions relatives à la protection des données sont soulevées, l'accès peut être donné au DPD de l'OLAF.

Une formation à la protection des données est prévue pour l'ensemble du personnel de l'OLAF pendant l'année 2008.

2.11.2. Le personnel de sécurité externe (et les gardes de sécurité en général) n'auront pas accès aux séquences de CCTV. À l'origine, le système de CCTV a été installé par l'entreprise privée qui l'a fourni. L'OLAF a conclu un contrat de maintenance technique avec cette entreprise. Aucune des opérations quotidiennes relatives à la CCTV n'a cependant été externalisée. Aucun garde de sécurité (qu'ils soient internes ou externes) n'aura accès au système de CCTV de l'OLAF.

En cas de panne technique nécessitant l'intervention d'experts techniques du fournisseur du système, l'accès aux vidéos stockées ou en direct par ces derniers sera limité au strict minimum nécessaire pour tester et vérifier que le système est de nouveau pleinement opérationnel à la fin de l'intervention. Le contractant a signé un accord général de non-divulgation pour l'ensemble du système, qui le lie, même après la fin du contrat. Chaque technicien travaillant sur le système devra également signer un accord de non-divulgation.

2.11.3. Accès aux séquences de CCTV; fichiers historiques et registres. Chacun des cinq agents de sécurité de l'OLAF aura un accès direct et pourra surveiller les séquences des caméras en direct à tout moment. Trois moniteurs seront installés: le premier dans le bureau du responsable local de la sécurité, le deuxième dans le bureau de son adjoint et le troisième dans celui des responsables de la sécurité de la gestion du réseau.

[1] Le responsable local de la sécurité (RLS) est le chef du secteur «Gestion Réseau et Sécurité» (GRS).

Ces systèmes sont protégés par un mot de passe. Le personnel de sécurité de l'OLAF se connecte et se déconnecte selon les besoins. Les agents se déconnectent lorsqu'ils laissent leur bureau sans surveillance. En outre, les portes sont fermées à clé et seront équipées d'un système de détection des intrusions. Chaque agent de sécurité de l'OLAF est techniquement en mesure de supprimer ou de copier une séquence de CCTV. Il ne peut cependant pas la modifier, sauf en l'exportant vers un DVD, comme précisé dans la section 2.13 ci-après.

Si un incident de sécurité est détecté ou suspecté, chaque agent de sécurité de l'OLAF peut décider individuellement s'il est nécessaire d'accéder aux séquences de CCTV (en direct ou enregistrées). Cette décision est justifiée dans un rapport sur tout incident suspecté ou confirmé au responsable local de la sécurité.

Il existe des fichiers historiques permettant de savoir qui a accédé, visionné, copié, modifié ou supprimé les séquences de CCTV. Les historiques du système sont exportés en temps quasi réel au «Core Business Information System's Security Information and Events Management System» (CBIS SIEMS en abrégé), qui consigne tous les événements relatifs à la sécurité de l'OLAF. L'historique du CBIS SIEMS ne peut pas être modifié. Le système est géré par les agents de sécurité de la gestion du réseau.

Hormis les fichiers historiques, il n'existe aucun registre électronique ou sur papier consignant l'accès aux séquences de CCTV. Cependant, comme susmentionné, l'accès est justifié dans les rapports sur les incidents suspectés ou confirmés remis au responsable local de la sécurité.

2.12. Transferts de données

2.12.1. Politique générale en matière de transferts. L'OLAF n'a pas de politique écrite officielle en ce qui concerne les autres personnes autorisées à accéder aux séquences de CCTV, hormis les agents de sécurité de l'OLAF, comme susmentionné.

L'OLAF a cependant expliqué au CEPD que toute demande serait gérée par le responsable du traitement, c'est-à-dire le chef de l'unité «Services de l'information» de l'OLAF, à la suite d'une consultation avec le DPD de l'OLAF. Elle sera documentée par une note dans le dossier.

En outre, toute demande d'accès aux séquences de CCTV sera gérée conformément

- aux articles 7, 8 ou 9 du règlement (CE) n° 45/2001,
- au règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, et
- aux articles 8 à 10 du règlement (CE) n° 1073/1999 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF).

La décision d'accorder l'accès ou non sera prise au cas par cas. En tout état de cause, aucun transfert systématique ou régulier n'est prévu.

2.12.2. Transferts au sein de l'OLAF. Le CEPD a demandé à l'OLAF de préciser dans quels cas le personnel de l'OLAF, autre que les agents de sécurité de l'OLAF ou les personnes concernées (par exemple, la direction ou les ressources humaines), peut avoir accès aux

données. L'OLAF a souligné que la décision serait prise au cas par cas, comme expliqué dans la section 2.12.1 ci-dessus.

2.12.3. Transferts à la Direction Sécurité de la Commission. L'OLAF n'a pas connecté son système de CCTV à celui géré par la Direction Sécurité de la DG ADMIN et n'envisage pas de le faire.

En effet, aucun accès n'est donné à la Direction Sécurité de la Commission directement ou en l'absence d'incident particulier. La Direction Sécurité n'a pas d'accès direct aux séquences de CCTV. La décision de lui donner cet accès si un incident de sécurité est détecté ou suspecté sera prise au cas par cas, comme expliqué dans la section 2.12.1 ci-dessus.

2.12.4. Transferts à l'Office d'investigation et de discipline de la Commission («IDOC»). L'OLAF peut transférer les séquences pertinentes (par exemple, celles qui peuvent servir de preuve) si l'IDOC les demande dans le cadre d'une enquête disciplinaire, en vertu des dispositions visées à l'annexe IX du Statut des fonctionnaires des Communautés européennes. La décision sera prise au cas par cas, comme expliqué dans la section 2.12.1 ci-dessus.

2.12.5. Transferts hors des institutions européennes. Le CEPD a également demandé à l'OLAF d'expliquer dans quels cas et dans le cadre de quelles procédures des tiers hors des institutions européennes (par exemple, la police belge, les tribunaux ou les médias) pourront avoir accès aux séquences de CCTV.

Plus particulièrement, le CEPD a demandé si l'OLAF exigeait une demande écrite signée par un fonctionnaire de police ou une ordonnance d'un tribunal émise par un juge, s'apparentant à un mandat pour perquisitionner une maison. Il a également demandé (i) si l'OLAF exigeait que la demande d'accès à la séquence de CCTV soit justifiée, (ii) si elle devait concerner une enquête particulière et (iii) remplir d'autres conditions.

Le CEPD a aussi spécifiquement demandé si les tribunaux traitant des affaires de droit civil, commercial, administratif ou du travail étaient autorisés à accéder aux séquences de CCTV. De plus, il a également demandé ce qu'il en était de l'accès aux séquences de CCTV (i) pour les parties défenderesses, si elles sont poursuivies pour un délit ou s'attendent à l'être, ou leurs avocats, et (ii) pour les parties impliquées dans une affaire de droit civil, commercial, administratif ou du travail (ou leurs avocats).

Dans sa réponse, l'OLAF a indiqué que toute demande de ce type devait être gérée au cas par cas. Pour les questions où des intérêts de la Communauté sont en jeu, l'OLAF s'inspirerait de l'ordonnance de la Cour de justice européenne dans l'affaire *Zwartveld e. a.*[2], indiquant qu'une demande d'accès à des informations présentée par le tribunal d'un État membre est régie par le principe de coopération loyale, qui impose des devoirs réciproques à cet égard. Si aucun enjeu communautaire n'est concerné, le droit belge s'appliquerait.

L'OLAF a également confirmé que si la police d'un État membre ou une autre organisation nationale demandait l'accès au cours d'une procédure officielle (c'est-à-dire hors du cadre du règlement (CE) n° 1049/2001 ou du règlement (CE) n° 45/2001), elle devrait d'abord obtenir une levée de l'immunité si la séquence concerne un membre du personnel de l'UE.

Enfin, l'OLAF a également confirmé estimer qu'il n'existe pas d'autre base juridique pour accorder l'accès aux parties privées que le règlement (CE) n° 1049/2001 ou les articles 7 à 9

[2] Affaire 2/88, Rec. 1990, p. I-3365.

et 13 du règlement (CE) n° 45/2001, et prévoit par conséquent que l'acceptation de ces demandes d'accès ne soit donnée que dans des circonstances très précises et rares. Toutes les demandes de ce type seront évaluées au cas par cas, comme expliqué dans la section 2.12.1 ci-dessus.

2.12.6. Modalités de transfert. Aucun accès direct ne sera accordé à quiconque ne faisant pas partie du personnel de sécurité de l'OLAF. Au contraire, les agents de sécurité de l'OLAF montreront aux destinataires autorisés les séquences de CCTV relatives au cas concerné. Ils pourront également fournir une copie de ces séquences sur un DVD.

2.13. Droits d'accès des personnes concernées. Si une personne concernée demande l'accès à ses données, l'OLAF prévoit de lui fournir une copie de la séquence sur un DVD ou de fixer un rendez-vous pour visionner les images de CCTV. La procédure pour soumettre une demande d'accès sera la suivante:

- la personne concernée peut demander l'accès aux images enregistrées la concernant à une date et un lieu déterminés; l'OLAF répondra dans un délai de 15 jours ouvrables;
- un agent de sécurité de l'OLAF visionnera la séquence pour déterminer si la personne concernée y apparaît;
- un rendez-vous sera pris avec la personne concernée pour visionner la vidéo; si la personne demande une copie de la séquence où elle apparaît, l'OLAF la lui donnera sur un DVD, sauf si l'une des exceptions visées à l'article 20 du règlement (CE) n° 45/2001 est applicable.

S'agissant des séquences gravées sur un DVD, les tiers non concernés par la demande particulière seront rendus anonymes grâce à un montage vidéo du module mpeg2 export effectué par un agent de sécurité de la gestion du réseau. Cependant, comme cela n'est pas toujours possible, le consentement des autres personnes concernées apparaissant sur la même séquence peut être requis. En cas de doute, le chef de l'unité «Services de l'information» de l'OLAF décide si cette séquence peut être donnée, en consultation avec le DPD.

La politique actuelle de l'OLAF prévoit de ne pas facturer la copie de la séquence.

2.14. Informations des personnes concernées. L'OLAF prévoit de fournir des informations détaillées aux personnes concernées sous différentes formes. En particulier, il

- publiera une déclaration sur le respect de la vie privée sur ses sites intranet et internet,
- mettra à disposition des brochures contenant le même texte à l'accueil du bâtiment, et
- fournira une information plus limitée sur place également.

2.14.1. Panneau sur le terrain. En ce qui concerne les informations sur place, des panneaux de taille A3 signalant la vidéosurveillance sont déjà présents à l'entrée principale. Ils concernent l'ancien système de CCTV. L'OLAF prévoit d'afficher le pictogramme ISO relatif à la vidéosurveillance à toutes les entrées du périmètre de sécurité de l'OLAF, en plus des panneaux dans l'entrée principale.

Sur les panneaux (à côté de chaque pictogramme), figureront les informations suivantes:

- le nom du responsable du traitement (OLAF),
- la finalité du traitement,
- le fait que les données sont enregistrées, et
- les informations de contact (adresse du site web).

2.14.2. Déclaration plus détaillée sur le respect de la vie privée pour le système de CCTV. L'OLAF a transmis une copie de son projet de déclaration sur le respect de la vie privée au CEPD. Le document de deux pages comprend les informations suivantes:

- une brève description de la couverture du système de CCTV (entrées et sorties, salles informatiques, etc.),
- la catégorie d'informations à caractère personnel collectées par le système de CCTV, la finalité et les moyens techniques utilisés,
- les personnes ayant accès aux séquences de CCTV,
- la manière dont l'OLAF protège les informations,
- la durée pendant laquelle l'OLAF conserve les données,
- la manière dont les personnes concernées peuvent vérifier, modifier ou supprimer leurs informations, et enfin,
- une mention soulignant le droit de recours auprès du CEPD.

2.14.3. Information régulière du personnel sur les plans de sécurité en cours. Enfin, l'OLAF a expliqué au CEPD que son personnel est régulièrement informé du plan de sécurité en cours depuis l'adoption de la politique de sécurité de l'information de l'OLAF. Cette information se fait (i) par la publication sur le site intranet de l'OLAF des décisions prises par les différentes commissions compétentes, (ii) par des présentations ad-hoc sur la sécurité aux groupes d'utilisateurs et (iii) par des introductions mensuelles sur la sécurité aux nouveaux venus. En outre, un courriel a été envoyé à l'ensemble du personnel le 1er février 2007, avant l'installation des trois nouveaux systèmes de contrôle physique, expliquant le travail en cours sur le nouveau système.

2.15. Mesures de sécurité

[...]

3. Analyse juridique

3.1. Contrôle préalable

3.1.1. Champ d'application de la notification. Comme mentionné à la section 2.1 du présent avis, le champ d'application de la notification et de cet avis concerne les aspects relatifs à la protection des données du système récemment installé de CCTV de l'OLAF, mais ne couvre pas celui de la Commission, qui fonctionne également dans le bâtiment de la Commission où se situe l'OLAF.

3.1.2. Applicabilité du règlement. Conformément à son article 3, le règlement (CE) n° 45/2001 s'applique

- au traitement de données à caractère personnel
- automatisé en tout ou en partie (ou au traitement de données à caractère personnel contenues dans un fichier), dans la mesure où
- ce traitement est mis en œuvre par les institutions et les organes communautaires
- pour l'exercice d'activités qui relèvent du champ d'application du droit communautaire.

Tous les éléments qui entraînent l'application du règlement (CE) n° 45/2001 sont réunis ici:

Premièrement, le fonctionnement du système de CCTV comprend la collecte et le traitement de données à caractère personnel, telles que définies à l'article 2, point a, du règlement. Deuxièmement, les données à caractère personnel collectées sont soumises à un «traitement automatisé», ainsi qu'à un traitement manuel et sont contenues dans un fichier (article 3, paragraphe 2, du règlement). En effet, les données à caractère personnel telles que les images des membres du personnel et des visiteurs sont automatiquement enregistrées et, dans certains cas, également surveillées en direct. Elles sont ensuite stockées en ligne et hors ligne et il est possible de les chercher en fonction de la date et du lieu. Certaines images peuvent également être récupérées, visionnées, copiées, modifiées et transférées à d'autres destinataires.

Troisièmement, le traitement est mis en œuvre par l'OLAF, un organe communautaire, et dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement).

Compte tenu de ce qui précède, le règlement (CE) n° 45/2001 est applicable.

3.1.3. Motifs de contrôle préalable. L'article 27, paragraphe 1, du règlement (CE) n° 45/2001 soumet au contrôle préalable du CEPD tous «les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités». L'article 27, paragraphe 2, contient une liste des traitements susceptibles de présenter de tels risques.

Étant donné qu'il s'agissait de son premier contrôle préalable concernant les systèmes de CCTV, le CEPD a dû analyser si ces systèmes en général, et celui de l'OLAF en particulier, présentent des risques particuliers, et doivent donc être soumis à un contrôle préalable.

Au cours de cette analyse, le CEPD a estimé que la vidéosurveillance est, de par nature, une technologie qui porte atteinte à la vie privée et dont l'abus est aisé. En outre, le recours répandu à la vidéosurveillance a également des impacts sociaux significatifs. D'autre part, le CEPD a également reconnu que tous les systèmes de CCTV ne présentaient pas le même niveau de risques pour le respect de la vie privée.

Le CEPD souligne tout d'abord que la vidéosurveillance, même si la séquence de CCTV n'est pas enregistrée, est très différente de la surveillance par des agents de sécurité sur le terrain. Contrairement à une ou plusieurs personnes en uniforme observant ouvertement leurs cibles à l'œil nu, dans le cas de la vidéosurveillance, la personne observée ne sait pas qui l'observe, ni pour quelle raison. Si les caméras ne sont pas installées à la vue de tous ou s'il n'y a pas d'information appropriée sur place, elle peut même ne pas avoir conscience d'être surveillée.

Sur le plan technique, les caméras de surveillance peuvent faire un gros plan sur une personne, enregistrer des images, les comparer dans une base de données d'images ou suivre des objets se déplaçant dans de grandes zones. Si les enregistrements sont conservés sur une longue période, il existe un risque accru de «détournement de la mission» («mission creep»), c'est-à-dire que les images soient utilisées à des fins non prévues et précisées à l'origine.

En outre, les images numériques peuvent également être facilement copiées et diffusées. Elles peuvent en effet être transmises à une multitude de destinataires ou publiées sur l'internet. Même si elles ne sont pas enregistrées par l'opérateur du système de CCTV et qu'elles sont seulement transférées aux destinataires prévus via un réseau interne, les images peuvent être interceptées par des pirates informatiques en cours de route ou enregistrées, puis utilisées à mauvais escient par l'un des destinataires.

Ces caractéristiques de la vidéosurveillance offrent de véritables possibilités de manquements à la sécurité et d'usages abusifs: la séquence peut tomber entre de mauvaises mains ou être utilisée par les destinataires légitimes à des fins illicites.

Les risques de la vidéosurveillance sont encore plus flagrants lorsque de réels abus se produisent. En effet, savoir que nos moindres faits et gestes sont surveillés par des caméras peut, en cas de surveillance répandue et continue, nous soumettre à un stress psychologique significatif, car nous devons en permanence adapter notre comportement aux attentes de ceux qui gèrent les caméras de surveillance. Cela constitue une intrusion importante dans notre vie privée, dont il faut peser le pour et le contre par rapport aux avantages qu'offre le recours à la CCTV.

De plus, la vidéosurveillance a également des impacts sociaux. Elle peut non seulement dissuader les activités criminelles, mais également toute autre forme de comportement anticonformiste.

En raison de ces considérations, le CEPD conclut que les systèmes de CCTV sont susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, au sens de l'article 27, paragraphe 1.

Cela dit, le CEPD souligne également que les caractéristiques et l'ampleur des systèmes de CCTV peuvent différer, en allant des plus petits et des plus simples aux plus grands, complexes et hautement sophistiqués, et des systèmes que l'on remarque à peine aux plus agressifs. Par conséquent, une analyse au cas par cas est nécessaire pour décider si un système de CCTV particulier doit être soumis à un contrôle préalable en vertu de l'article 27, paragraphe 1.

En ce qui concerne le système de CCTV proposé par l'OLAF, la version finale des lignes directrices sur la vidéosurveillance n'étant pas disponible, le CEPD a décidé de procéder à un contrôle préalable du système, afin d'aider l'OLAF à être en pleine conformité. En outre, sur une question essentielle, la durée de la période de conservation, les plans de l'OLAF décrits dans la notification différaient de manière significative de ceux qui seront recommandés par le CEPD dans ses lignes directrices. Cela confirme également que le contrôle préalable des plans de l'OLAF peut apporter une valeur supplémentaire et aider à garantir une plus grande conformité aux exigences en matière de protection des données.

3.1.4. Notification et date de remise de l'avis du CEPD. La notification a été reçue le 17 octobre 2007. En vertu de l'article 27, paragraphe 4, du règlement (CE) n° 45/2001, cet avis doit être rendu dans un délai de deux mois. La procédure a été suspendue pendant 153 jours au total. Par conséquent, l'avis doit être rendu le 19 mai 2008 au plus tard (18 décembre 2007 + suspension pendant 110 jours + 14 jours + 29 jours pour commentaires).

3.1.5. Véritable contrôle préalable. Le traitement a été notifié au CEPD après l'installation du système de CCTV, mais avant que le responsable du traitement ne mette le système en service. Le CEPD a publié son avis le 19 mai 2008.

Dans la mesure où le contrôle préalable est conçu pour faire face aux situations susceptibles de présenter des risques, l'avis du CEPD devrait normalement être demandé et donné avant le début du traitement. Le CEPD se réjouit d'avoir été consulté avant que l'OLAF ne mette en service son nouveau système de CCTV et que le DPD de l'OLAF ait été impliqué dans la décision relative à ce système à un stade précoce.

Dans ce cas, comme cela sera indiqué aux sections 3.2 et 3.4 ci-après relatives à la licéité et à la proportionnalité, le CEPD a conclu que la finalité du système de CCTV de l'OLAF est licite et que l'ampleur et l'installation du système (matériels et logiciels informatiques et ressources humaines) sont proportionnées. Par conséquent, toutes les recommandations formulées par le CEPD afin d'améliorer la conformité en ce qui concerne le respect de la vie privée peuvent être mises en œuvre sans démonter ou changer l'emplacement des caméras de CCTV, ni procéder à des adaptations coûteuses du système. Étant donné que cela n'est pas toujours le cas pour tous les systèmes de CCTV notifiés, le CEPD encourage des notifications précoces (avant l'installation et l'investissement dans le système) ou une implication étroite du DPD à la décision dès le début.

3.2. Licéité du traitement. L'article 5, point a, du règlement (CE) n° 45/2001 dispose que les données à caractère personnel ne peuvent être traitées que si «le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités […] ou d'autres actes législatifs adoptés sur la base de ces traités».

La première question au titre de l'article 5, point a, est de déterminer s'il existe une base légale particulière pour le traitement: une disposition du traité ou un autre acte législatif adopté sur la base des traités. La seconde question consiste à déterminer si le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public. Pour répondre à cette seconde question dans le cas présent, le considérant 27 du règlement doit être pris en considération: «le traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes». Ainsi, la seconde question en l'espèce est de savoir si le traitement est nécessaire et proportionné pour la gestion et le fonctionnement de l'OLAF.

Base légale. En ce qui concerne la première question, la notification énumère un certain nombre de documents comme base légale des opérations de CCTV:

- l'article 297 du traité CE;
- l'article 17 du Statut des fonctionnaires;
- le règlement (CE) n° 1073/1999 du Parlement européen et du Conseil, du 25 mai 1999, relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF): considérants 4, 17 et 18; articles 8, 11, paragraphe 1, et 12, paragraphe 3;
- la décision 1999/352/CE, CECA, Euratom de la Commission du 28 avril 1999 instituant l'Office européen de lutte antifraude (OLAF): considérants 4 et 5; article 2, paragraphe 5, et article 3;
- la décision 2001/844/CE, CECA, Euratom de la Commission du 29 novembre 2001 modifiant son règlement intérieur: dispositions relatives à la sécurité;
- la décision de la Commission du 16 août 2006 C(2006) 3602 relative à la sécurité des systèmes d'information (disponible à l'adresse suivante: http://intracomm.cec.eu-admin.net/security/legislation/legislation_en.htm);
- la politique relative à la sécurité des systèmes d'information de la Commission (actuellement en cours de révision, obsolète, version non-officielle de 2001 disponible à: http://intracomm.cec.eu-admin.net/security/legislation/legislation_en.htm); et
- la politique relative à la sécurité de l'information de l'OLAF (section 4.5 du manuel de l'OLAF[3]).

[3] La dernière version du manuel de l'OLAF est celle du 25 février 2005. Un nouveau manuel est en cours de préparation.

Parmi ces documents, les quatre premiers ne sont qu'indirectement pertinents pour le système de CCTV de l'OLAF. Par contre, les quatre derniers documents énumérés par l'OLAF concernent directement les mesures de sécurité que l'OLAF peut prendre afin de sécuriser l'accès physique non autorisé à ses locaux, infrastructures informatiques et informations opérationnelles, ce qui correspond à l'objectif des opérations de CCTV de l'OLAF.

Néanmoins, aucun de ces documents ne requiert spécifiquement l'installation d'un système de CCTV afin de garantir la sûreté et la sécurité des opérations de l'OLAF. En effet, ces documents ne mentionnent que très peu souvent la CCTV[4]. À la demande du CEPD, l'OLAF a confirmé ne pas avoir non plus adopté lui-même de document sur la CCTV à l'OLAF spécifiquement. À la connaissance de l'OLAF, la Commission ou sa Direction Sécurité n'a pas non plus adopté de document portant spécifiquement sur la CCTV.

Par conséquent, les actes législatifs spécifiques adoptés sur la base des traités ne fournissent pas de conditions détaillées sur le fonctionnement du système de CCTV de l'OLAF. Le CEPD considère toutefois que les documents plus généraux énumérés constituent une base légale suffisante pour l'installation et le fonctionnement du système de CCTV de l'OLAF.

Cela dit, le CEPD estime souhaitable que l'OLAF adopte des lignes directrices internes

- décrivant les objectifs, le cadre et l'utilisation de son système de CCTV et
- prévoyant des garanties pour la protection des données déjà en place ou recommandées dans cet avis.

Proportionnalité. En ce qui concerne la seconde question à analyser pour examiner la licéité du système de CCTV de l'OLAF, le CEPD est également convaincu et ne conteste pas que le traitement notifié soit nécessaire et proportionné pour la gestion et le fonctionnement de l'OLAF. Le CEPD a fondé ses conclusions sur la proportionnalité principalement sur les faits suivants:

- les objectifs du système sont clairement définis, relativement limités et légitimes: le principal objectif du système de CCTV de l'OLAF est la protection contre l'accès physique non autorisé, notamment aux informations opérationnelles sensibles et à l'équipement informatique;
- l'emplacement, la couverture et la résolution, ainsi que les autres aspects de l'installation du système de CCTV semblent adéquats, pertinents et non excessifs par rapport aux objectifs définis, compte tenu également du caractère sensible des informations détenues par l'OLAF: en particulier, les caméras ne sont situées qu'à proximité des entrées et sorties de la zone sécurisée de l'OLAF et à certains autres endroits stratégiques, comme certaines salles

[4] L'OLAF a expliqué que la section 18.3.8 de la décision 2001/844/CE de la Commission dispose que «Lorsque des systèmes d'alarme, des circuits fermés de télévision et d'autres dispositifs électriques sont utilisés pour protéger des informations classifiées de l'UE, des systèmes de secours doivent être prévus pour permettre leur fonctionnement permanent en cas de rupture de l'alimentation électrique principale. Il est, en outre, fondamental que tout défaut de fonctionnement ou toute tentative de neutralisation des systèmes précités déclenche une alarme ou soit signalé par tout autre moyen fiable au personnel de surveillance». L'OLAF a confirmé que ces deux exigences étaient remplies avec le système de CCTV de l'OLAF. Toutes les parties du système de CCTV sont protégées par un système d'alimentation non interruptible (UPS) et le «Security Information and Events Management System» (SIEMS) centralise les alarmes de tous les systèmes.

informatiques non surveillées et le centre de gestion des documents de l'OLAF.

Le CEPD émet cependant la réserve suivante: certains aspects du traitement disproportionnés devront être modifiés. Cela s'applique en particulier à la période de conservation, qui sera abordée à la section 3.5 ci-après.

En outre, le CEPD attire également l'attention de l'OLAF sur le fait qu'avant d'activer la fonction d'enregistrement du son des caméras de son nouveau système de contrôle d'accès, il doit (i) mettre en place des garanties pour la protection des données et (ii) demander l'avis préalable du CEPD. Jusque là, la fonction d'enregistrement du son doit être éteinte ou désactivée d'une autre manière. En tout état de cause, le CEPD souligne que la CCTV ne doit pas être utilisée pour écouter ou enregistrer des conversations entre deux personnes du public, car il s'agit d'une méthode très agressive et qui a peu de chance de se justifier.

Pour conclure, le CEPD considère que le traitement notifié est licite, si les recommandations formulées dans cet avis sont suivies.

3.3. Traitement portant sur des catégories particulières de données. Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle sont interdits, à moins que des motifs ne soient trouvés à l'article 10, paragraphes 2 à 4, du règlement (CE) n° 45/2001.

Le CEPD souligne tout d'abord que les séquences de CCTV révèlent par nature certaines indications sur l'origine raciale ou ethnique des personnes filmées par les caméras. C'est inévitable, et s'il n'existe pas d'autres facteurs de risques, cela ne signifie pas que le traitement doit être interdit comme relevant de l'article 10 du règlement.

En l'espèce,

- l'OLAF n'a pas l'intention de collecter et de traiter des données sensibles;
- des données sensibles ne seraient filmées par les caméras que très rarement et tout à fait incidemment. En particulier, aucun établissement médical, religieux ou syndical n'est situé au sein de la zone couverte par le système de CCTV et il est également improbable que des manifestants passent dans le champ de vision des caméras;
- la sécurité du système de CCTV interne, les garanties prises pour la protection des données et le nombre limité de destinataires (cinq agents de sécurité) suggèrent que le risque que des données sensibles tombent entre de mauvaises mains ou soient utilisées abusivement est relativement limité.

Par conséquent, le CEPD conclut que l'article 10 n'interdit pas à l'OLAF d'installer et d'utiliser son système de CCTV selon ses plans décrits dans cet avis. Cela dit, le CEPD recommande que la formation à la protection des données dispensée au personnel de sécurité de l'OLAF mette particulièrement en exergue le fait que les données traitées peuvent, dans certains cas, être considérées comme des données sensibles et qu'il convient donc d'être particulièrement vigilant en les sauvegardant. La formation doit également expliquer qu'au cours d'une enquête sur des incidents de sécurité, le personnel ne doit pas établir le profil des personnes filmées par les caméras sur la base de leur appartenance à une religion particulière ou de leur origine raciale ou ethnique.

3.4. Qualité des données

Adéquation, pertinence et proportionnalité. Conformément à l'article 4, paragraphe 1, point c, du règlement (CE) n° 45/2001, les données à caractère personnel doivent être «adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement».

Outre les questions relatives à la durée de la période de conservation, qui seront abordées à la section 3.5, à partir des informations qui lui ont été fournies, le CEPD ne conteste pas l'adéquation, la pertinence et la proportionnalité de l'installation et du fonctionnement du système de CCTV de l'OLAF. Cela dit, le CEPD souligne que la conformité à ces trois principes demande toujours une analyse «in concreto», au cas par cas.

Loyauté et licéité. L'article 4, paragraphe 1, point a, du règlement (CE) n° 45/2001 dispose que les données doivent être traitées loyalement et licitement. La question de la licéité a été analysée ci-dessus (cf. section 3.2). Celle de la loyauté est étroitement liée au type d'informations fournies aux personnes concernées (cf. section 3.8 ci-après).

Exactitude. Conformément à l'article 4, paragraphe 1, point d, du règlement, les données à caractère personnel doivent être «exactes et, si nécessaire, mises à jour» et «toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées».

Sur la base des informations fournies, le CEPD ne conteste pas l'exactitude des données vidéo collectées par le système de CCTV de l'OLAF. En particulier, l'OLAF a confirmé que la résolution de ses caméras était suffisante pour fournir des images faciales reconnaissables. En outre, il a également confirmé que les caméras sont installées et orientées de manière à obtenir des images pertinentes permettant d'identifier les personnes à l'origine d'un incident de sécurité. La date et le lieu sont également indiqués sur la séquence.

3.5. Conservation des données

Le principe général du règlement (CE) n° 45/2001 est le suivant: les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement (article 4, paragraphe 1, point e, du règlement).

Le CEPD est d'avis que les arguments avancés par l'OLAF au cours de cette procédure de contrôle préalable pour justifier la proportionnalité d'une période de conservation d'un an sont insuffisants. À partir des faits en l'espèce, le CEPD a estimé que la période de conservation d'un an prévue par l'OLAF est excessive.

Tous les incidents de sécurité mentionnés par l'OLAF au CEPD pour illustrer ses besoins en matière de sécurité et justifier la nécessité du système de CCTV concernaient des accès physiques non autorisés aux locaux de l'OLAF et potentiellement à ses informations opérationnelles sensibles.

Ces incidents de sécurité seraient ou devraient généralement être détectés immédiatement, par une alerte, ou, tout au plus, dans un délai de quelques jours. Par exemple, la porte d'une salle sécurisée laissée ouverte accidentellement à la fin de la journée serait ou devrait être

découverte le lendemain matin au plus tard. Les deux autres systèmes de contrôle d'accès physique de l'OLAF devraient être surveillés régulièrement et, d'après les informations du CEPD, le sont effectivement; toute intrusion ou panne du système devrait être détectée presque instantanément.

Si ce n'est pas le cas, au lieu d'allonger de manière disproportionnée la période de conservation des séquences de CCTV au cas où un incident de sécurité ne serait découvert qu'après plusieurs mois ou années, l'OLAF devrait s'efforcer d'améliorer ses capacités de prévention et de détection des incidents de sécurité.

La possibilité théorique que la divulgation d'un document opérationnel ne soit découverte que plusieurs années après son accès illicite et que dans un tel cas le visionnage a posteriori de plusieurs années de séquences de CCTV permette de trouver qui aurait pu divulguer le document n'est pas suffisante pour justifier la proportionnalité de conserver toutes les séquences de CCTV pendant un an, voire plus.

Le CEPD souligne également que, dans les pays européens où la législation ou les autorités nationales responsables de la protection des données prévoient une période de conservation maximale autorisée, cette période est généralement d'un mois au maximum. En fait, les séquences de CCTV utilisées à des fins de sécurité sont généralement effacées et écrasées en l'espace de quelques jours, ce qui est normalement suffisant pour détecter tout accès non autorisé, vol ou autre activité criminelle qui pourrait être filmé par les caméras.

Compte tenu de ce qui précède, le CEPD recommande à l'OLAF de réévaluer la nécessité de conserver toutes les séquences de CCTV pour une période d'un an. Ce faisant, il convient de garder à l'esprit que les périodes de conservation doivent correspondre étroitement aux périodes durant lesquelles l'accès aux données à caractère personnel peut être nécessaire à des fins clairement définies. L'OLAF devrait en particulier estimer combien de temps il doit conserver les données afin de révéler qu'un accès physique non autorisé a effectivement eu lieu. Le CEPD recommande que les séquences de CCTV soient effacées dans un délai de quelques jours ou semaines, la période de conservation exacte devant être décidée en fonction de l'évaluation interne des besoins effectuée par l'OLAF.

3.6. Destinataires et transferts de données

Le CEPD salue le fait que les destinataires prévus soient limités aux cinq agents de sécurité de l'OLAF, comme décrit à la section 2.11.3 ci-dessus.

Compte tenu du fait qu'un historique du système approprié est conservé (comme décrit à la section 2.11.3 ci-dessus), le CEPD estime acceptable que l'ensemble des cinq agents de sécurité de l'OLAF puisse visionner et copier les séquences de CCTV. Cependant, le CEPD recommande à l'OLAF de réexaminer ce point pour savoir s'il ne serait pas suffisant que seul un nombre plus limité de personnes au sein de l'équipe de sécurité aient la possibilité technique de modifier et de supprimer des séquences de CCTV. Par exemple, la possibilité de procéder à des opérations pourrait être limitée au responsable local de la sécurité et à son adjoint.

Le CEPD considère également que le transfert ad hoc de données à la Direction Sécurité de la DG ADMIN et à l'IDOC, soumis aux garanties décrites par l'OLAF à la section 2.12 ci-dessus, est conforme à l'article 7, paragraphe 1, du règlement (CE) n° 45/2001, qui se lit comme suit: les données à caractère personnel ne peuvent faire l'objet de transferts entre institutions ou organes communautaires ou en leur sein que si elles sont nécessaires à

l'exécution légitime de missions relevant de la compétence du destinataire. Le CEPD souligne que, conformément à l'article 7, paragraphe 3, les destinataires traitent les données à caractère personnel reçues de l'OLAF uniquement aux fins qui ont motivé leur transmission.

Le CEPD salue également l'engagement de l'OLAF qui ne permettrait des transferts de données non prévus demandés par un tiers (au sein ou à l'extérieur de l'OLAF) que si le règlement (CE) n° 45/2001 l'autorise spécifiquement. Le CEPD se félicite particulièrement qu'en cas de doute, le chef de l'unité «Services de l'information» de l'OLAF consulte le DPD de l'OLAF avant de procéder au transfert de données demandé.

3.7. Droit d'accès et de rectification

Droit d'accès. Conformément à l'article 13, point c, du règlement (CE) n° 45/2001, la personne concernée a le droit d'obtenir, sans contrainte, du responsable du traitement la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données. L'article 20 prévoit certaines limitations à ce droit, notamment lorsqu'une telle limitation constitue une mesure nécessaire pour garantir la protection de la personne concernée ou des droits et libertés d'autrui.

Le CEPD se réjouit que l'OLAF ait confirmé qu'il donnerait l'accès aux séquences de CCTV aux personnes concernées, si elles le demandent. Le CEPD salue également les mesures prises par l'OLAF afin de garantir

- que toute demande d'accès soit traitée en temps utile (dans les quinze jours),
- sans contrainte (les demandes d'accès n'ont pas besoin d'être justifiées) et
- que les droits des tiers soient protégés par un recours au montage ou à une demande de consentement.

Le CEPD se félicite également que le chef de l'unité «Services de l'information» consulte le DPD de l'OLAF, s'il souhaite limiter l'accès à des données demandées.

Droit de rectification. L'article 14 du règlement confère à la personne concernée le droit de rectifier les données inexactes ou incomplètes. En raison de la nature des séquences de CCTV, il est relativement peu probable que les personnes concernées aient besoin de rectifier leurs données, même s'il est toujours possible que la date ou l'emplacement de la séquence soit erroné ou que le rapport rédigé par le personnel de sécurité sur un incident de sécurité indique erronément la personne concernée ou contienne d'autres erreurs. Le CEPD recommande que l'OLAF prenne des garanties analogues à celles appliquées au droit d'accès afin de garantir que les personnes concernées puissent exercer en toute confiance leur droit de rectification, si nécessaire.

3.8. Information des personnes concernées

Les articles 11 et 12 du règlement exigent que certaines informations soient communiquées aux personnes concernées afin de garantir la transparence du traitement des données à caractère personnel. L'article 11 est applicable aux données collectées auprès de la personne concernée, tandis que l'article 12 s'applique aux cas où les données n'ont pas été collectées auprès de la personne concernée. Par conséquent, c'est l'article 12 qui s'applique aux séquences de CCTV.

Publication et format de l'information relative à la protection des données. L'article 12 dispose que les informations doivent être fournies lorsque les données sont enregistrées ou communiquées pour la première fois, sauf si la personne est déjà informée.

Dans ses lignes directrices sur la vidéosurveillance, le CEPD recommandera l'association des trois méthodes suivantes pour la diffusion de l'information:

- l'affichage d'avis sur les murs des bâtiments ou les barrières pour prévenir les passants de la surveillance en cours et leur donner les principales informations sur le traitement,
- la publication sur l'internet d'une déclaration détaillée sur le respect de la vie privée pour les personnes souhaitant en savoir davantage sur les pratiques de vidéosurveillance, et
- la mise à disposition, sur demande, d'une version sur papier de la même déclaration à l'accueil du bâtiment.

La mise à disposition d'informations plus détaillées sur l'internet et à l'accueil ne doit pas se substituer aux avis affichés à l'extérieur des bâtiments. Au contraire, elles doivent les compléter. Les avis affichés à l'extérieur doivent comprendre autant d'informations énumérées à l'article 12 que cela semble raisonnable dans le cas d'espèce. En tout état de cause, ils doivent au moins mentionner l'identité du responsable du traitement et la finalité de la surveillance. Ils doivent également indiquer clairement que les images ne sont pas uniquement regardées, mais également enregistrées, fournir des informations de contact et préciser que des informations supplémentaires sont disponibles sur l'internet et à l'accueil du bâtiment.

Le personnel de sécurité et de l'accueil doit être formé aux aspects relatifs au respect de la vie privée des pratiques de vidéosurveillance et pouvoir faire immédiatement des copies, sur demande, de la déclaration détaillée sur le respect de la vie privée. Il doit également être en mesure d'indiquer aux personnes concernées à qui s'adresser si elles ont des questions supplémentaires ou souhaitent demander l'accès à leurs données.

L'emplacement et la taille des panneaux doivent être prévus afin que les personnes concernées puissent les voir et les lire avant d'entrer dans la zone surveillée.

Le CEPD salue les bonnes pratiques de l'OLAF consistant à fournir les informations requises sur la protection des données en ligne, à la fois sur les sites web interne et externe de l'OLAF. Les personnes concernées (le personnel de l'OLAF, ainsi que les visiteurs externes) sont rassurées de savoir que leurs données seront traitées de manière loyale et licite. Le CEPD se félicite également de la pratique de l'OLAF, qui fournit les mêmes informations, sur demande, à l'accueil du bâtiment. Enfin, le CEPD est satisfait de l'augmentation prévue du nombre de panneaux actuellement affichés sur place, ainsi que de la révision du contenu et de l'ajout d'informations.

En effet, l'OLAF semble suivre de près les recommandations qui seront intégrées aux lignes directrices sur la vidéosurveillance. Afin de garantir la pleine conformité, le CEPD attire l'attention de l'OLAF sur le fait que la formation à la protection des données prévue par l'OLAF pour l'ensemble de son personnel en 2008 devrait comprendre la formation particulière des réceptionnistes et des gardes de sécurité, comme mentionné ci-dessus.

Contenu de l'information sur la protection des données. L'article 12 du règlement (CE) n° 45/2001 donne une liste détaillée d'informations à communiquer aux personnes

concernées. Essentiellement, le responsable du traitement doit leur indiquer l'identité de la personne qui procède au traitement, les catégories de données concernées et les finalités du traitement. Ces informations doivent également préciser les origines et les destinataires des données, si les réponses sont obligatoires ou facultatives et prévenir les personnes concernées de l'existence d'un droit d'accès aux données et de rectification. D'autres informations, notamment la base juridique du traitement, les délais de conservation des données et le droit de saisir le CEPD, doivent également être fournies si elles sont nécessaires pour assurer un traitement loyal des données. Cela peut dépendre des circonstances du cas d'espèce.

Enfin, l'article 12 permet certaines exceptions à l'obligation d'information. Étant donné (i) qu'aucune des exceptions visées à l'article 12 ne s'applique aux faits de l'espèce et (ii) que tous les éléments énumérés à l'article 12 (y compris la base juridique du traitement, les délais de conservation des données et le droit de saisir le CEPD) sont nécessaires pour assurer un traitement loyal, le CEPD estime que tous les éléments énumérés à l'article 12 doivent être indiqués dans l'information sur la protection des données, à l'exception des «origines des données» et de la mention «réponses obligatoires ou facultatives», éléments évidents dans le cas d'espèce.

Le CEPD salue le fait que l'information sur la protection des données comprend une brève indication sur tous les éléments, sauf un, requis à l'article 12 du règlement. Le CEPD recommande que l'élément manquant (base juridique) soit ajouté à la déclaration sur le respect de la vie privée, après que l'OLAF aura adopté le document interne recommandé à la section 3.2 ci-dessus.

Le CEPD souligne qu'il accorde une importance particulière à ce que le texte de l'avis sur la protection des données soit clair, concis, facile à lire et évite tout jargon inutile sur la protection des données.

Recommandations supplémentaires. Le CEPD aborde ci-après uniquement les éléments énumérés à l'article 12 pour lesquels il suggère d'autres modifications.

Informations sur le droit d'accès. Le CEPD recommande de ne pas se contenter ici de mentionner uniquement l'existence de ce droit et de fournir des informations de contact, mais de préciser également:

- les délais fixés dans cet avis (quinze jours),
- la manière dont l'OLAF donnera cet accès (visionnage ou copie sur un DVD),
- la manière dont il protègera les droits des tiers (montage ou consentement), et
- le fait que l'OLAF ne prévoit pas de faire payer ce droit d'accès.

Destinataires. Les informations fournies par l'OLAF au cours de la procédure de contrôle préalable suggèrent que les gardes de sécurité n'ont pas accès à toutes les séquences de CCTV. L'information sur le respect de la vie privée devrait être adaptée en conséquence.

Référence à l'avis du CEPD. Le CEPD recommande en outre que l'information sur le respect de la vie privée fasse référence et renvoie à cet avis sur le site web du CEPD.

3.9. Sécurité. Conformément à l'article 22 du règlement, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger. Ces mesures sont prises notamment afin d'empêcher toute

diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération, ainsi que toute autre forme de traitement illicite.

Le CEPD remarque que les infrastructures informatiques particulières de l'OLAF font l'objet d'un examen horizontal du CEPD dans une procédure distincte. Le rôle de cet avis sur le contrôle préalable n'est pas de refaire cet examen. Cela dit, le CEPD a évalué les informations supplémentaires que l'OLAF a fournies spécifiquement en ce qui concerne son système de CCTV. Au cours de cet examen, le CEPD n'a pas découvert d'éléments qui feraient douter de l'adéquation des mesures de sécurité prises par l'OLAF afin d'assurer la sécurité de ses séquences de CCTV.

Conclusion

Rien ne permet de conclure à un manquement aux dispositions du règlement (CE) n° 45/2001, sous réserve qu'il soit pleinement tenu compte des considérations formulées aux sections 3.2 à 3.9. Les recommandations du CEPD concernent essentiellement les points suivants:

- base légale:
  - l'OLAF devrait adopter un document interne décrivant son système de CCTV et prévoyant des garanties appropriées pour la protection des données;

- conservation des données:
  - l'OLAF devrait revoir la période de conservation prévue afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire aux fins initialement envisagées;

- information des personnes concernées:
  - des informations plus spécifiques et exactes doivent être fournies aux personnes concernées, quant à certains éléments énumérés à l'article 12 du règlement.

En outre, le CEPD souligne qu'avant d'activer la fonction d'enregistrement du son des caméras de son nouveau système de contrôle d'accès, l'OLAF doit (i) mettre en place des garanties pour la protection des données et (ii) demander l'avis préalable du CEPD. Jusque là, la fonction d'enregistrement du son doit être éteinte ou désactivée d'une autre manière. En tout état de cause, la CCTV ne doit pas être utilisée pour écouter ou enregistrer des conversations entre deux personnes du public, car il s'agit d'une méthode très agressive et qui a peu de chance de se justifier.

Fait à Bruxelles, le 19 mai 2008

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données