Avis sur la notification d'un contrôle préalable reçue du délégué à la protection des données de la Cour des comptes concernant le contrôle de l'Internet

Bruxelles, le 10 novembre 2008 (Dossier 2008-284)

1. Procédure

Le 26 novembre 2007, le Contrôleur européen de la protection des données (ci-après le «**CEPD**») a formulé des commentaires sur la politique de sécurité de l'Internet (ci-après la «**PSI**») de la Cour des comptes. Les commentaires du CEPD ont été émis en réponse à la demande d'évaluation émanant de la Cour des comptes (ci-après la «**Cour**»), conformément à l'article 46, point d), du règlement (CE) n° 45/2001 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 (ci-après le «**règlement (CE) n° 45/2001**» ou le «**règlement**»). Dans ses commentaires, le CEPD demandait notamment à la Cour des comptes de lui transmettre une notification de contrôle préalable en rapport avec le contrôle par la Cour de son infrastructure de technologies de l'information et de la communication, c'est-à-dire l'infrastructure Internet (ci-après «**ICTI**» ou «**Internet**»).

En réponse à la demande du CEPD, le délégué à la protection des données de la Cour des comptes a transmis, le 6 mai 2008, une notification pour contrôle préalable (ci-après «**la notification**») concernant le traitement de données relatif au contrôle ICTI réalisé par la direction Informatique et télécommunications de la Cour (ci-après «**direction IT**»).

Le 3 juillet 2008, le CEPD a adressé au délégué à la protection des données (ci-après le «**DPD**») de la Cour une demande en vue de confirmer et de clarifier certaines informations factuelles concernant les pratiques de contrôle de la Cour. Le CEPD a reçu une réponse le 9 juillet 2008.

Le 11 juillet 2008, le CEPD a transmis à la Cour un projet d'avis sur le contrôle préalable pour commentaire.

Le 3 septembre 2008, un contact téléphonique a eu lieu entre le CEPD et la Cour afin de discuter des recommandations contenues dans le projet d'avis sur le contrôle préalable envoyé à la Cour pour commentaire. À la demande de la Cour, le délai de présentation des commentaires a été reporté jusqu'au 29 septembre 2008, date à laquelle lesdits commentaires ont effectivement été reçus.

Les commentaires transmis par la Cour ont apporté des changements importants aux procédures de contrôle de la Cour. Le 29 septembre 2008, le CEPD a prolongé d'un mois le délai d'adoption de son avis afin d'examiner les nouvelles pratiques de contrôle. Le même jour, le CEPD a demandé à la Cour des éclaircissements sur certains aspects des nouvelles procédures de contrôle. La Cour a

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

transmis les informations demandées le 2 octobre 2008. Le 3 novembre 2008, le délai d'adoption de l'avis a été prolongé de quinze jours supplémentaires.

2. Examen de l'affaire

Le présent avis évalue le degré de conformité des activités de traitement de données liées au contrôle ICTI de la Cour avec le règlement (CE) n° 45/2001. Cet avis n'analyse pas les autres opérations de traitement de données pouvant découler de procédures administratives et disciplinaires susceptibles d'être engagées à la suite de violations alléguées de la PSI de la Cour.

Les activités de traitement de données de la Cour analysées dans cet avis sont décrites dans la notification, dans la PSI de la Cour des comptes, adoptée par le Secrétaire général de la Cour le 29 janvier 2008, dans la procédure de contrôle de l'Internet (ci-après la «**PCI**»), qui doit être adoptée, et dans la Foire aux questions (ci-après la «**FAQ**»). Le traitement de données proprement dit visant le contrôle des utilisateurs de l'ICTI de la Cour n'a pas encore entamé.

2.1. Les faits

Le traitement des données consiste essentiellement dans le contrôle de l'utilisation de l'Internet par les utilisateurs de l'ICTI de la Cour. Les ***objectifs du traitement*** des données sont multiples et portent notamment sur les éléments suivants: *i)* identifier les ressources ICTI utilisées à tout instant afin de déterminer celles qui gênent le trafic normal; *ii)* résoudre les problèmes, par exemple lorsque l'accès à l'Internet n'est pas possible ou est lent; *iii)* analyser l'efficacité des filtres de sécurité afin de vérifier si le filtre de contenu n'est pas trop restrictif ou trop souple. En outre, le traitement vise également à *iv)* vérifier que les utilisateurs de la Cour utilisent l'ICTI conformément aux usages autorisés par la PSI de la Cour. Afin d'éviter les répétitions, les objectifs *i), ii)* et *iii)* peuvent se résumer en un seul, à savoir «assurer la fonctionnalité du réseau et éviter les failles dans la sécurité».

La direction IT est ***responsable du traitement des données*** et certaines opérations de traitement de données sont réalisées par des membres de cette direction (administrateurs de système). Cependant, une part importante du traitement des données sera effectuée par le responsable de la sécurité des TI, qui ne fait pas rapport à la direction IT, mais bien au directeur de l'administration et des finances. Il importe également d'observer que la responsabilité de la PSI relève de la direction des ressources humaines. Compte tenu du partage des responsabilités en matière de politiques de contrôle de l'Internet et des pratiques de traitement des données en place, trois directions générales sont concernées et l'on peut affirmer que le rôle de responsable du traitement des données est exercé conjointement par les trois directions. De ce fait et dans le souci d'éviter les répétitions, le présent avis désignera sous le terme générique «la Cour» les trois entités qui contrôlent conjointement le traitement des données et qui sont donc les responsables du traitement des données.

Les ***catégories de données à caractère personnel*** qui doivent être collectées et traitées ultérieurement incluent toutes les tentatives d'accès à l'Internet (réussies et ratées), qui sont d'abord consignées et ensuite analysées. Les informations qui seront consignées sont notamment les suivantes: *i)* identification de l'utilisateur; *ii)* volume des données échangées par l'Internet (en Ko); *iii)* date et heure de la tentative d'accès à l'Internet; *iv)* adresse IP de l'ordinateur; *v)* temps de traitement de la demande Internet; *vi)* catégorie de filtre de contenu; *vi)* résultat du filtre de contenu; *vii)* numéro de PC; *x)* URL consultés; *xi)* réponse à la demande et *xii)* numéro du port TCP/IP. Enfin, le journal des échecs de connexion apportera des informations sur la cause de l'impossibilité d'accéder à l'Internet (erreurs de réseau, noms de sites incorrects, expirations de session, adresses Internet inconnues, tentatives d'accéder à des sites protégés par un filtre, etc.).

Les ***traitements manuels et automatisés de données*** sont étroitement liés. Bien que certaines opérations de traitement de données comme la collecte initiale de l'information soient automatiques, cette information est ensuite traitée par des administrateurs de système et par le responsable de la sécurité des TI selon la procédure décrite ci-après.

Premièrement, la direction IT enregistrera systématiquement *toutes* les tentatives d'accès à l'Internet des utilisateurs de l'ICTI de la Cour. Le contenu des informations consignées comprend les données à caractère personnel décrites plus haut sous le point intitulé «Catégories de données à caractère personnel».

Deuxièmement, des *administrateurs de système* examineront le contenu des fichiers journaux à tout moment lorsque: *i)* un problème technique survient et *ii)* un ou plusieurs indicateurs de performance indiquent une valeur inhabituelle. Ils peuvent signaler les événements inhabituels ou les activités suspectées d'être illicites ou contraires à la PSI au responsable de la sécurité des TI.

Troisièmement, à la fin de chaque mois, le *responsable de la sécurité des TI* analysera les fichiers journaux enregistrés au cours du mois écoulé. Cette analyse repose sur les fichiers journaux de l'ensemble du personnel de la Cour et comprend les échecs de connexion à l'Internet. L'analyse aura pour but *i)* d'assurer la fonctionnalité du réseau et d'éviter les failles dans la sécurité et *ii)* de vérifier si les utilisateurs de la Cour emploient l'ICTI conformément aux usages autorisés par la PSI de la Cour. Cette analyse aboutit à un rapport sur l'utilisation de l'Internet. Ce rapport contiendra des informations sur les éléments suivants:

i) volume et pourcentage d'utilisation des différents protocoles Internet (HTTP, HTTPS, FTP, etc.);
ii) volume et pourcentage d'utilisation des différents types de fichier (fichiers de texte, exécutables, multimédias, etc.);
iii) nombre d'erreurs pendant une période donnée et classement des erreurs par type (dues à des problèmes de réseau, à des problèmes d'identification, à l'authentification, à des filtres);
iv) classement des quatre erreurs de filtre par raison (filtré par qu'il s'agissait de sites Internet ou de types de fichiers non autorisés ou illégaux) et distribution par période;
v) en fonction des résultats du point précédent, distribution par adresse IP ou par identité d'utilisateur au cours d'une période donnée;
vi) évaluation d'un échantillon de 100 historiques (y compris les URL) afin de déterminer s'ils représentent un danger pour l'ICTI de la Cour;
vii) contrôle visuel d'une vingtaine d'endroits différents du fichier journal afin de voir s'il est possible de dégager des tendances particulières (caractères répétitifs, caractères spéciaux, etc.). Chaque résultat sera commenté et recevra une note qualitative («pas de risque», «risque faible», «risque moyen» ou «risque élevé») et une explication de la manière dont cette note a été attribuée, mentionnant les références contre les logiciels malveillants, la législation, les politiques, les normes, les informations sur la sécurité provenant de sources fiables, etc.;
viii) calcul des valeurs d'utilisation de l'Internet; la plus faible, la plus élevée, la moyenne;
ix) examen des sites ou du trafic dangereux mentionnés par le SANS, le CERT ou tout autre bulletin d'information d'un organisme d'alerte;
x) examen des URL extrêmement longs qui ont été consultés;
xi) liste des 150 sites Internet les plus consultés;
xii) distribution du trafic Internet en nombre de visites et en volume par catégorie (sport, économie, science, jeux).

Quatrièmement, le rapport sera envoyé au directeur des ressources humaines (ci-après le «**DRH**») pour analyse. Selon la classification des risques, le DRH pourra décider de demander des informations supplémentaires au responsable de la sécurité des TI. Par exemple, par combien de personnes, au cours de quelle période et combien de fois un site Internet dangereux a-t-il été

consulté ou une tentative d'y accéder a-t-elle eu lieu. L'objectif est de déterminer si une personne ou un groupe de personnes essaie délibérément de contourner les filtres, accède ou tente d'accéder à un ou plusieurs sites Internet non autorisés (matériel pornographique, xénophobie, etc.) ou à des sites Internet qui pourraient endommager l'ICTI de la Cour (pracking, warez, crackz, etc.).

Au vu des résultats de l'analyse, le DRH décidera de lever ou non l'anonymat de la ou des personnes soupçonnées d'utiliser l'ICTI de manière non autorisée. L'intéressé sera invité à fournir des explications et le DRH décidera de lancer ou non une enquête administrative et une procédure disciplinaire.

Les personnes concernées sont toutes les personnes qui utilisent les services Internet à la Cour des comptes, à savoir le personnel de la Cour, les experts et les stagiaires ainsi que les employés travaillant pour des prestataires de services extérieurs ou toute autre personne utilisant l'infrastructure de technologie de l'information et de la communication de la Cour (ci-après les «utilisateurs», les «utilisateurs de l'Internet», les «utilisateurs de l'ICTI» et le «personnel de la Cour»).

En ce qui concerne la ***conservation des données***, selon la notification, les fichiers journaux sont supprimés six mois après avoir été collectés.

Le responsable du traitement de données peut ***transférer des données à caractère personnel*** aux types de destinataires suivants: *i)* le directeur des ressources humaines; *ii)* les enquêteurs internes et *iii)* l'OLAF.

En ce qui concerne le ***droit à l'information***, la notification indique que les utilisateurs ont été officiellement informés de la PSI et de la procédure de contrôle de l'Internet (PCI) par un avis officiel et par la publication de la PSI, de la PCI et de la FAQ sur l'Intranet de la Cour des comptes.

En outre, lors de sa première connexion à l'Internet, l'utilisateur doit confirmer qu'il a lu et compris la PSI. Des copies de l'avis officiel d'adoption de la politique de sécurité de l'Internet, de la foire aux questions et de la procédure de contrôle de l'Internet ont été jointes à la notification ou fournies ultérieurement au cours de la période fixée pour les commentaires.

Conformément à la PCI, le ***droit d'accès*** est garanti aux personnes concernées. Selon les informations reçues, le ***droit de rectification*** ne s'applique pas, puisque les données sont collectées automatiquement.

Des ***mesures de sécurité*** sont mises en oeuvre: [....]

2.2. Les aspects juridiques

2.2.1. Contrôle préalable

Le présent avis porte sur le traitement de données par la Cour des comptes en vue du contrôle de l'utilisation de l'ICTI de la Cour. En conséquence, cet avis examine la mesure dans laquelle les opérations de traitement de données décrites plus haut et effectuées par la Direction IT et par le responsable de la sécurité des TI sont conformes au règlement (CE) n° 45/2001.

Applicabilité du règlement. Le règlement (CE) n° 45/2001 s'applique au «*traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*» et au traitement «*par toutes les institutions et organes communautaires, dans la mesure où ce traitement est mis en*

œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire». Pour les motifs énoncés ci-après, toutes les conditions d'application du règlement sont réunies.

Premièrement, le contrôle de l'utilisation de l'Internet implique la collecte et le traitement ultérieur de *données à caractère personnel* telles qu'elles sont définies à l'article 2, point a), du règlement (CE) n° 45/2001. En effet, comme l'indique la notification, les données à caractère personnel des utilisateurs de l'Internet sont collectées et traitées ultérieurement. Cela couvre l'identification de l'utilisateur, les adresses IP, les URL consultés, la date et l'heure, le contenu, etc.

Deuxièmement, comme l'indique la notification, les données à caractère personnel collectées subissent des opérations de «*traitement automatisé*» au sens de l'article 2, point a), du règlement (CE) n° 45/2001, ainsi que des opérations de traitement manuel des données. En effet, les informations personnelles sont d'abord collectées de manière automatisée directement auprès des utilisateurs de l'Internet (enregistrement automatique des fichiers journaux) et analysées ensuite par le responsable de la sécurité des TI.

Enfin, le traitement est réalisé par une institution communautaire, en l'espèce la Cour des comptes, dans le cadre du droit communautaire (article 3, paragraphe 1, du règlement (CE) n° 45/2001). Par conséquent, toutes les conditions d'application du règlement sont réunies dans le traitement de données aux fins du contrôle de l'Internet.

Raisons d'effectuer un 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, du règlement dresse une liste des traitements susceptibles de présenter de tels risques. Cette liste inclut, au point a), «*les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, (…)*» et au point b), «*les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement*».

Compte tenu, d'une part, du fait que le contrôle de l'utilisation de l'Internet tel qu'il est décrit dans la PSI mène à l'évaluation du comportement des utilisateurs (afin d'évaluer si leur utilisation de l'Internet est ou non conforme à la PSI) et, d'autre part, du fait que ce contrôle peut impliquer la collecte de données relatives à des suspicions (en cas de suspicion d'un comportement illicite) ainsi que d'autres types de données sensibles, ce contrôle et les opérations de traitement de données qui en découlent doivent, en principe, faire l'objet d'un contrôle préalable en application de l'article 27, points a) et b), du règlement (CE) n° 45/2001.

Notification et date prévue pour l'avis du CEPD. La notification a été reçue le 6 mai 2008. Le délai dans lequel le CEPD doit rendre son avis conformément à l'article 27, paragraphe 4, du règlement (CE) n° 45/2001 a été prolongé d'un mois en raison des changements importants apportés au traitement de données au cours du délai initial de deux mois et a ensuite été prolongé de quinze jours supplémentaires. La procédure a également été suspendue durant le mois d'août. Le délai dans lequel le CEPD doit rendre son avis a été suspendu pendant un total de 58 jours afin d'obtenir des informations factuelles supplémentaires et de permettre à la Cour de formuler des commentaires sur le projet d'avis du CEPD. Par conséquent, le CEPD doit rendre son avis au plus tard le 18 novembre 2008.

2.2.2. Licéité du traitement

Le traitement de données à caractère personnel ne peut être effectué que si l'un des motifs visés à l'article 5 du règlement (CE) n° 45/2001 existe. Selon la notification, parmi les divers motifs visés à l'article 5, ceux qui justifient le traitement se fondent sur l'article 5, point a), selon lequel le

traitement des données peut être effectué si le traitement est «*nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités*».

Pour déterminer si les traitements sont conformes à l'article 5, point a), du règlement (CE) n° 45/2001, deux éléments doivent être pris en compte: premièrement, si le traité ou d'autres actes législatifs prévoient une mission d'intérêt public sur la base de laquelle le traitement des données est effectué (*base juridique*) et, deuxièmement, si les traitements sont effectivement nécessaires à l'exécution de cette mission, c'est-à-dire à la réalisation des objectifs poursuivis (*nécessité*).

Base juridique. Les actes législatifs qui justifient le traitement des données par la Cour des comptes sont indiqués ci-après.

Premièrement, le CEPD observe que la Cour des comptes a adopté une PSI. Celle-ci énonce, notamment, les règles d'utilisation de l'Internet afin d'assurer le bon usage du système d'information et de communication de la Cour. La PSI prévoit le contrôle de l'utilisation de l'Internet, en ce compris l'enregistrement de chaque tentative d'accès à l'Internet effectuée par les utilisateurs de l'ICTI de la Cour afin d'assurer la fonctionnalité du réseau et une utilisation de l'ICTI conforme aux usages autorisés par la PSI. En somme, l'adoption de cette politique et sa communication aux utilisateurs de l'ICTI de la Cour constituent pour le CEPD un élément pertinent pour déterminer s'il existe une base juridique adéquate au sens de l'article 5, point a), du règlement (CE) n° 45/2001.

Deuxièmement, le CEPD note que la législation existante sur la protection des données, à savoir le règlement (CE) n° 45/2001, contient plusieurs dispositions justifiant le contrôle de l'utilisation d'Internet dans certains buts qui coïncident avec les objectifs poursuivis par le contrôle de la Cour. En particulier, le considérant 30 du règlement (CE) n° 45/2001 dispose ce qui suit: «*Il peut être nécessaire de contrôler les réseaux d'ordinateurs fonctionnant sous la responsabilité des institutions et organes communautaires en vue de prévenir un usage non autorisé*». Comme indiqué plus haut, l'un des objectifs poursuivis par la Cour en mettant en place un contrôle de l'Internet est de prévenir un usage de celui-ci qui soit contraire aux règles énoncées dans la PSI. De même, l'article 37, paragraphe 2, du règlement (CE) n° 45/2001 ajoute un motif supplémentaire autorisant la Cour à procéder à un traitement de données très spécifique, à savoir conserver les données relatives au trafic, en l'occurrence les fichiers journaux. En particulier, l'article 37, paragraphe 2, dispose que les données relatives au trafic peuvent être traitées, aux fins de la gestion du budget des télécommunications et du trafic, y compris la vérification de l'usage autorisé des systèmes de télécommunication. La notion de «*vérification de l'usage autorisé*» est essentielle, dans la mesure où elle concerne l'usage éventuel de données relatives au trafic en dehors de la gestion du budget et du trafic. Elle permet notamment l'utilisation de données relatives au trafic pour assurer la sécurité du système ou des données et le respect du statut ou d'autres dispositions, telles que celles contenues dans la politique de sécurité de l'Internet. Dans ce cas précisément, le contrôle a lieu pour vérifier que les utilisateurs se servent de l'ICTI de la Cour pour les usages autorisés par celle-ci dans sa PSI. Dans ce contexte, un élément clé, discuté plus avant au point 2.2.4, consiste à déterminer dans quelle mesure un contrôle est nécessaire pour vérifier un usage autorisé. Le CEPD est d'avis qu'un usage autorisé peut être déterminé de différentes façons. Il peut être déterminé en termes de volume (taille du document téléchargé), du temps passé sur la Toile ou des sites consultés. Un usage autorisé peut également être déterminé par d'autres moyens, comme des plaintes émanant de tiers, un rendement inhabituellement bas d'un membre du personnel, etc.

Enfin, le CEPD observe que la Cour des comptes, en sa qualité d'employeur, a certains droits et obligations en matière de droit du travail, qui peuvent être considérés comme des motifs juridiques adéquats justifiant le traitement. Ainsi, le droit de la Cour de se protéger contre la responsabilité du

dommage que les actes des travailleurs peuvent causer peut également justifier le traitement. Cela inclut le traitement de données sensibles dans certaines circonstances (voir le point 2.2.3).

Nécessité. Comme indiqué plus haut, la nécessité du traitement de données est directement liée à l'objectif que ce traitement entend atteindre. En d'autres termes, la nécessité du traitement de données dépend des objectifs poursuivis par le traitement considéré. En l'espèce, pour évaluer cette nécessité, il convient de tenir compte du degré de nécessité de l'enregistrement de l'utilisation de l'Internet et de l'analyse ultérieure des fichiers journaux (ces deux éléments formant le «contrôle») par rapport aux objectifs mentionnés dans la politique de sécurité de l'Internet.

Comme indiqué plus haut, l'un des principaux objectifs du traitement dans le cadre du contrôle de l'Internet consiste à vérifier si les utilisateurs de la Cour utilisent l'ICTI conformément aux usages autorisés dans la PSI de la Cour. Le CEPD est d'avis que si la Cour ne met pas en place un certain contrôle de l'utilisation de l'ICTI, il est probable qu'elle ne préviendra pas un usage de l'ICTI contraire à sa PSI. En effet, à défaut d'un tel contrôle, la Cour ne peut pas détecter les usages non autorisés et ne sera pas en mesure de les empêcher. Par conséquent, il semble que l'enregistrement des fichiers journaux et leur analyse, à tout le moins dans une certaine mesure, sont nécessaires à l'exécution de la mission consistant à assurer un usage de l'Internet conforme à la politique de sécurité de l'Internet et, partant, la sécurité globale de l'ICTI de la Cour. Le CEPD considère également que pour atteindre le second objectif de la politique de sécurité de l'Internet, c'est-à-dire assurer la fonctionnalité du réseau et éviter les failles dans la sécurité, la Cour doit procéder à un traitement des données. L'enregistrement de l'accès à l'Internet et un certain degré de contrôle sont nécessaires pour permettre à la Cour d'identifier les ressources de l'ICTI utilisées à tout moment et de résoudre les problèmes. Enfin, un certain contrôle est également nécessaire pour permettre à l'employeur, en l'occurrence la Cour, d'exercer, le cas échéant, ses droits et obligations en matière de droit du travail. À titre d'exemple, si la Cour n'était pas en mesure de contrôler l'utilisation de l'Internet par une personne soupçonnée d'avoir un comportement contraire à la PSI (par exemple, le téléchargement de pornographie), elle ne disposerait pas des preuves nécessaires pour engager une procédure disciplinaire.

Compte tenu de ce qui précède, le CEPD est d'avis que le contrôle de l'ICTI de la Cour est nécessaire à la réalisation des objectifs poursuivis par cette dernière. Par conséquent, le CEDP est convaincu que les exigences de conformité avec l'article 5, point a), du règlement (CE) n° 45/2001 sont en principe satisfaites.

Cela étant, il convient de relever qu'un contrôle généralisé ou un contrôle très approfondi de l'utilisation de l'Internet par chaque utilisateur, par rapport à un contrôle plus sélectif (par exemple, en cas de suspicion), n'est pas nécessaire à tout instant. Dès lors, si la Cour met en place ce type de contrôle généralisé ou très approfondi, elle peut ne pas disposer des motifs visés à l'article 5, point a), du règlement (CE) n° 45/2001 pour le réaliser. C'est la raison pour laquelle, dans le cadre de l'évaluation de la nécessité, il est plus juste de dire qu'un «***certain***» contrôle est nécessaire pour se conformer à l'article 5, point a), du règlement (CE) n° 45/2001. Le point **2.2.4** ci-dessous propose certaines limitations aux procédures de contrôle de la Cour, de sorte que seul un contrôle réellement nécessaire ait lieu, conformément au «principe de qualité des données».

2.2.3. Traitement portant sur des catégories particulières de données

Le contrôle de l'utilisation de l'Internet peut révéler des données à caractère personnel «sensibles». Ces données sont définies par le règlement comme 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 les données relatives à la santé ou à la vie sexuelle*» (article 10). Ainsi, l'appartenance syndicale peut être révélée en accédant à des historiques qui font

apparaître un accès officiel régulier au site Internet d'un syndicat particulier. L'accès à certains sites Internet peut indiquer des préférences sexuelles. Le traitement de données sensibles est, en principe, interdit à moins que l'un des motifs visés à l'article 10 du règlement (CE) n° 45/2001 justifiant le traitement existe.

L'article 10, paragraphe 2, point b), du règlement (CE) n° 45/2001 dispose que l'interdiction ne s'applique pas lorsque le traitement est «*nécessaire afin de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités*».

Un certain contrôle de l'usage de l'Internet peut être jugé nécessaire par la Cour afin d'assurer la sécurité du système ou des données et le respect du statut et d'autres dispositions. Ceci inclut le respect des droits et obligations en matière de droit du travail. Cela couvrirait, par exemple, l'obligation faite à la Cour d'empêcher que des informations sexuellement offensantes soient regardées sur le lieu de travail, une obligation qui justifierait le traitement par la Cour d'informations sensibles, telles que certains URL consultés susceptibles de révéler qu'un employé se livre à ce type d'activité. Le contrôle des informations sensibles peut également se justifier dans certains cas pour permettre à l'employeur d'exercer ses droits en tant qu'employeur, comme le droit d'engager des procédures disciplinaires aboutissant au licenciement d'employés se livrant à des activités illicites, telles que regarder et télécharger du matériel promouvant des actes criminels. En conclusion, le CEPD considère qu'en sa qualité d'employeur, la Cour des comptes est soumise aux droits et aux obligations en matière de droit du travail qui justifient un traitement par la Cour des données sensibles des utilisateurs de l'ICTI, qui ne peut être évité (voir le point 2.2.4 «*Collecte des URL consultés*» pour des considérations supplémentaires).

2.2.4. 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. C'est ce que l'on appelle le principe de qualité des données.

A priori, le CEPD considère que, dans l'ensemble, les données enregistrées dans les fichiers journaux semblent adéquates au regard des finalités du traitement. Cependant, pour les deux catégories suivantes d'informations collectées dans les fichiers journaux, le CEPD doute que leur traitement en vue de déterminer si les utilisateurs de la Cour emploient l'ICTI conformément aux usages autorisés soit conforme au principe de qualité.

Fichiers journaux des échecs de connexion à l'Internet. Le CEPD note que la Cour enregistre *tous* les fichiers journaux, sans exception. Le CEPD comprend que, pour des raisons techniques, afin d'assurer la fonctionnalité du réseau et d'éviter des failles dans la sécurité, y compris pour le débogage, l'identification des erreurs DNS, etc., la Cour doive enregistrer les échecs de connexion à l'Internet. Le CEPD considère que ce traitement est conforme au principe de qualité des données.

Il observe toutefois que la Cour *utilise* ces journaux non seulement pour assurer la fonctionnalité du réseau et éviter des failles dans la sécurité, mais également afin de déterminer si des utilisateurs se servent l'ICTI de la Cour à des fins autorisées. En particulier, le responsable de la sécurité des TI classe les erreurs de filtre en fonction des raisons qui déclenchent le filtre (filtrage parce que le site Internet ou le type de fichier n'est pas autorisé ou est illicite) et analyse la période où le filtre a été activé (c'est-à-dire quand il s'est enclenché). Sur la base des résultats de cette analyse, le responsable de la sécurité des TI relie chaque échec de connexion à l'Internet à l'adresse IP ou à

l'identifiant de l'utilisateur qui a effectué la tentative.

Le CEPD rappelle qu'il existe des technologies pour réduire la nécessité d'un contrôle général et exhaustif de *toutes* les tentatives d'accès à l'Internet. Parmi celles-ci figure le logiciel de filtrage, qui filtre l'accès aux sites Internet préalablement classés comme inappropriés ou illicites. Le CEPD note que la Cour utilise un logiciel de filtrage et d'autres techniques afin de limiter l'accès à des informations inappropriées, comme les données obscènes, racistes, offensantes au plan religieux ou sexuel, ce dont le CEDP se félicite. L'utilisation de ces techniques sous-entend une approche préventive contre l'usage abusif de l'Internet plutôt qu'une approche répressive ou d'investigation. En outre, ces techniques sont plus respectueuses de la vie privée, parce qu'elles rendent inutile ou, à tout le moins, réduisent considérablement la nécessité de contrôler les échecs de visualisation des informations bloquées. En effet, si la personne ne réussit jamais à accéder et à visualiser le contenu d'un site Internet bloqué donné, il ne semble pas y avoir une nécessité légitime d'enregistrer cet échec.

Sur ce point, le CEPD est désagréablement surpris par le fait que, tout en utilisant un logiciel de filtrage, la Cour ne profite pas de cette technologie pour réduire la nécessité de contrôler l'accès à l'Internet sur son ICTI.

De l'avis du CEPD, l'adoption simultanée des deux approches, à la fois préventive (logiciel de filtrage) et répressive ou d'investigation (contrôle) peut sembler *excessive*, à la fois en termes de traitement et de collecte des données, et peut enfreindre le principe de qualité des données.

Au vu de ce qui précède, le CEPD invite la Cour à ***reconsidérer*** son approche du contrôle des échecs de connexion à l'Internet ou de produire des motifs légitimes. Si la Cour devait conclure, sur la base de motifs sains, qu'il est nécessaire d'analyser les échecs de connexion à l'Internet, le CEPD invite la Cour à mettre au moins en place les mesures de sauvegarde suivantes et à l'en informer:

i) il convient d'élaborer une politique qui fixe un pourcentage d'utilisation du filtrage (activation du filtre), par période, par personne réputée normale; en d'autres termes, il y a lieu de déterminer ce qui est un nombre normal d'échecs de connexion par personne. Lors que l'utilisation du filtrage est supérieure au seuil susvisé, la politique doit permettre au responsable de la sécurité des TI de contrôler les échecs de connexion à des sites Internet. Par exemple, si l'utilisation de filtres est supérieure à 10 par personne, la onzième activation du filtre permettra au responsable de la sécurité des TI de relier les échecs de connexion à l'identifiant de l'utilisateur ou à l'adresse IP d'où est partie la demande de connexion;

ii) étant donné les conséquences potentielles de la mise en correspondance des échecs de connexion avec une adresse IP ou un identifiant d'utilisateur, le CEPD considère que, pour que le traitement soit loyal, certaines informations doivent être transmises à l'utilisateur de l'ICTI. Le CEPD est notamment d'avis que la Cour devrait mettre en place un système envoyant automatiquement un message électronique ou ouvrant une fenêtre contextuelle, par exemple, après un certain nombre d'échecs de connexion à l'Internet, afin d'informer l'utilisateur qu'en raison du nombre élevé d'échecs (au cours d'une période donnée), le responsable de la sécurité des TI pourrait renforcer le contrôle de son utilisation de l'ICTI. Cela s'applique bien évidemment sans préjudice des informations sur les procédures de contrôle fournies dans la PCI.

***Contrôle des URL consultés*.** Comme indiqué plus haut, le CEPD est conscient que la collecte d'URL est nécessaire pour assurer la fonctionnalité du réseau et éviter les failles dans la sécurité. Les URL consultés révèlent non seulement des données relatives au trafic, mais également le contenu spécifique qui a probablement été visualisé, y compris des données sensibles. La Cour traite les URL consultés afin d'assurer la fonctionnalité du réseau, mais aussi pour évaluer l'usage abusif des TIC de la Cour. Cette évaluation est réalisée en analysant chaque mois un échantillon de

100 historiques pour l'ensemble du personnel. Le résultat de cette analyse est une liste indiquant le niveau de risque («pas de risque», «risque faible», «risque moyen» ou «risque élevé») pour l'ICTI de la Cour.

Dans ce contexte, deux questions essentielles se posent. **Premièrement**, la mesure dans laquelle le ***contrôle des URL*** est nécessaire aux fins de l'évaluation de la conformité avec la PSI doit être déterminée. En d'autres termes, pour être conforme au principe de qualité des données, comment et jusqu'à quel point le contrôle des URL doit-il être réalisé? **Deuxièmement**, s'il existe une suspicion fondée qu'une personne commet un abus (révélé par un contrôle ou par d'autres moyens hors connexion), ***quelles sont les mesures procédurales*** à prendre pour garantir qu'un contrôle accru potentiel de ce comportement n'est pas excessif et que seules sont menées les actions de contrôle nécessaires à la réalisation des objectifs poursuivis?

Sur le premier point (**contrôle sans suspicion ou utilisation d'indicateurs**), le point de vue du CEPD peut se résumer comme suit:

i) en l'absence de suspicion fondée, le contrôle de *tous* les URL consultés par *tous* les utilisateurs est jugé inutile et excessif; cela vaut en particulier lorsque le contrôle touche l'ensemble du personnel. En l'absence de suspicion, même un contrôle limité de manière aléatoire paraît inutile. C'est le cas, par exemple, des contrôles indirects tels que celui proposé par la Cour et consistant à contrôler des échantillons de 100 historiques d'URL par mois. De l'avis du CEPD, cette pratique est évitable parce que, ainsi qu'on le verra, il existe d'autres moyens moins intrusifs, comme l'utilisation d'autres types d'indicateurs, qui peuvent faire apparaître des comportements suspects et rendre ainsi inutile le contrôle complet ou même limité de manière aléatoire des URL, qui est une pratique plus intrusive;

ii) le CEPD concède que, dans certains cas, la Cour peut devoir contrôler les URL consultés par *certaines* personnes. Ainsi, lorsqu'il existe une *suspicion fondée* qu'un utilisateur adopte un comportement contraire à la PSI (par exemple, le téléchargement d'images pédophiles), il est clair que la collecte d'informations relatives aux URL consultés par cet utilisateur est adéquate dans la mesure où elle aidera à prouver que l'utilisateur concerné a adopté ce comportement;

iii) il peut être dérogé au principe énoncé sous le point i), par exemple, parce que le danger associé à des URL extrêmement longs prime sur l'intrusion dans la vie privée qu'implique leur contrôle[1]. Par conséquent, le CEPD considère que leur contrôle, qui établit un lien entre ce type d'URL et l'identifiant des utilisateurs ou les adresses IP, n'est pas excessif. Le même raisonnement s'applique aux sites ou au trafic dangereux, tels qu'ils sont définis par le SANS, le CERT ou tout autre bulletin d'information d'organismes d'alerte;

iv) Outre le contrôle des longs URL, la Cour peut utiliser d'autres indicateurs pour détecter les abus. Le CEPD conseille à la Cour de recourir à ces indicateurs. Parmi ceux-ci figurent la collecte d'informations sur le volume de données téléchargées, le temps passé sur l'Internet, ainsi que d'autres facteurs qui ne passent pas par le contrôle des URL (collecte de suspicions déclenchées par d'autres moyens en ligne, par exemple un rendement inhabituellement bas). Comme indiqué plus haut, les schémas d'activation des filtres peuvent jouer le même rôle. Pour utiliser ces indicateurs, la Cour devrait élaborer des schémas d'usage et des écarts par rapport à l'usage. À cet égard, les schémas d'usage fondés sur le volume peuvent se révéler plus pratiques que d'autres, comme le

[1] Des URL excessivement longs peuvent être un indice d'une tentative d'attaque par URL, par laquelle le pirate informatique se sert de la barre d'adresse d'Internet Explorer pour pirater le site.

temps passé sur l'Internet, dans la mesure où certaines tâches nécessitent des recherches sur la Toile et peuvent donc susciter de fausses suspicions. En élaborant des schémas d'usage fondés sur le volume (ou tout autre critère pertinent), la Cour devrait veiller à ne pas aboutir à un contrôle et à une surveillance disproportionnés.

***En résumé,* le CEPD considère que l'utilisation de logiciels de filtrage, la collecte d'informations sur le temps passé sur l'Internet, éventuellement la collecte des échecs de connexion à l'Internet (sous réserve des mesures de sauvegarde précitées) ainsi que d'autres indicateurs hors connexion devraient suffire à la direction IT et au responsable de la sécurité des TI pour atteindre les objectifs de contrôle sans passer par un contrôle des URL, hormis dans des cas limités.**

En l'espèce, le CEPD se félicite tout particulièrement que la Cour ne contrôle pas *tous* les URL de *tous* les utilisateurs. Le CEPD juge que le fait que la Cour se fonde sur des indicateurs comme le volume de données téléchargées et le pourcentage d'utilisation des protocoles Internet et de certains types de fichiers est positif. Le CEPD déplore toutefois que la Cour envisage de contrôler des échantillons de 100 historiques d'URL par mois et juge cette pratique inutile. Par conséquent, il invite la Cour à ***reconsidérer*** cette pratique ou à fournir d'autres justifications.

Par ailleurs, il convient de tenir compte du fait que le contrôle des URL peut faire apparaître des informations sensibles. Comme cela a été discuté au point 2.2.3, la Cour dispose de motifs légitimes pour traiter des informations sensibles dans le cadre de l'exercice de ses droits et obligations en matière de droit du travail. Ces motifs peuvent notamment exister lorsque la Cour souhaite exercer certains droits et obligations découlant du droit du travail, comme le lancement d'une procédure disciplinaire fondée sur une suspicion qu'un utilisateur commet un acte répréhensible. Dans ces cas, le contrôle peut être nécessaire pour ouvrir une enquête administrative ou engager une procédure disciplinaire contre l'utilisateur visé. Cependant, en l'absence de suspicion ou d'exercice de droits et obligations découlant du droit du travail, les motifs légitimes justifiant la collecte de ce type d'informations ne sont pas évidents. C'est un argument supplémentaire en faveur de la collecte limitée des URL consultés lorsqu'une suspicion d'acte répréhensible existe sur la base d'indicateurs et/ou de moyens hors connexion.

En ce qui concerne la seconde question (**contrôle en cas de suspicion**), le point de vue du CEPD peut se résumer comme suit:

i) dès qu'il existe dans le chef du responsable de la sécurité des TI une suspicion fondée qu'une personne commet un abus (sur la base des critères ci-dessus), le CEPD suggère la mise en place d'une politique consistant à accroître progressivement le contrôle en fonction des circonstances. Cela permettra d'éviter que le contrôle soit excessif, puisque seules seront traitées les données nécessaires à la réalisation des objectifs poursuivis. Dans ce contexte, il est important de rappeler que, étant donné que les URL sont toute manière collectés et enregistrés à des fins techniques, en cas de suspicion de comportement répréhensible, le responsable de la sécurité des TI pourra toujours analyser les URL conservés dans les fichiers journaux de la personne dont le comportement est suspect;

En d'autres termes, dans la pratique, pour procéder à un contrôle supplémentaire lorsque le responsable de la sécurité des TI nourrit une suspicion fondée d'usage non autorisé, une procédure doit être mise en place qui détermine quand, comment et dans quelles conditions ce contrôle supplémentaire sera réalisé. Pour ce faire, le CEPD formule les suggestions suivantes;

ii) la découverte de suspicions grâce à l'application des critères ci-dessus peut être jugée suffisamment pertinente pour justifier l'étape suivante, qui consiste à rapporter la suspicion à la

hiérarchie sans révéler l'identité de la personne concernée. Dans ce cas, la Cour envisage de transmettre chaque mois des rapports au directeur des ressources humaines, qui peut révéler les comportements suspects. Le CEPD est satisfait de cette pratique. Le rapport n'est pas censé révéler l'identité de l'utilisateur. Dans ce contexte, le CEPD suggère de supprimer tout identifiant ou adresse IP susceptible d'être relié à l'utilisateur;

iii) les informations sur le comportement suspect doivent permettre à la personne compétente, en l'occurrence le DRH, de demander un contrôle approfondi de la personne suspectée, par exemple, pendant deux à quatre semaines. À la fin des deux ou quatre semaines, le responsable de la sécurité des TI doit transmettre un nouveau rapport confirmant ou invalidant la suspicion. En principe, aucune action ne doit être prise avant la confirmation de la suspicion par ce contrôle ciblé supplémentaire.

En l'espèce, il est prévu que le rapport du responsable de la sécurité des TI permettra au DRH, après avoir informé le DPD, de décider si des informations supplémentaires sont nécessaires. Sur la base des résultats de l'analyse, le DRH décidera de lever ou non l'anonymat de la personne soupçonnée d'utiliser l'ICTI d'une manière contraire aux usages autorisés par la PSI. Cette personne sera invitée à fournir des explications et le DRH décidera ensuite de lancer ou non une enquête administrative et une procédure disciplinaire. Le CEPD considère que cette procédure est adéquate.

Loyauté et licéité. L'article 4, paragraphe 1, point a), du règlement dispose que les données à caractère personnel doivent être traitées loyalement et licitement. La licéité a été examinée plus haut (voir point 2.2.2). La loyauté est étroitement liée au type d'informations fournies aux personnes concernées. Cette question est abordée plus en détail au point 2.2.8.

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*». En l'espèce, les données incluent les fichiers journaux. La direction IT doit prendre toutes les mesures raisonnables pour garantir que les données sont mises à jour et pertinentes. Voir aussi le point 2.2.8.

2.2.5. Conservation des données

Conformément à l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001, 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 et/ou pour lesquelles elles sont traitées ultérieurement.

Selon la notification et la PSI, les fichiers journaux sont effacés six mois après leur collecte. Six mois doivent être un délai maximal. Cela est conforme à l'article 37 du règlement (CE) n° 45/2001, qui prévoit des mesures spécifiques pour la conservation des données relatives au trafic et à la facturation et les fichiers journaux sont inclus dans cette définition. L'article 37, paragraphe 2, du règlement prévoit que les données relatives au trafic peuvent être traitées aux fins de la gestion du budget et du trafic, y compris la vérification de l'usage autorisé des systèmes de télécommunications. Cependant, ces données doivent être effacées ou rendues anonymes dès que possible et, au plus tard, six mois après leur collecte, à moins que leur conservation ultérieure soit nécessaire à la constatation, à l'exercice ou à la défense d'un droit dans le cadre d'une action en justice en instance devant un tribunal.

Si le contrôle des fichiers journaux conduit la Cour à soupçonner une personne d'avoir enfreint la PSI, la Cour est autorisée à conserver les fichiers journaux incriminant la personne suspectée afin

de constater, d'exercer ou de défendre un droit dans le cadre d'une action en justice en instance devant un tribunal. Il est à noter que cette mesure ne doit être prise qu'au cas par cas, lorsqu'il existe une suspicion légitime qu'une personne a enfreint la PSI ou le statut et que la Cour a ouvert une enquête administrative. Dans ce contexte, l'article 20 du règlement est également pertinent en ce qu'il prévoit des limitations possibles au principe d'effacement immédiat des données visées à l'article 37, paragraphe 1, notamment lorsque la limitation constitue une mesure nécessaire pour «*assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales*». Par conséquent, si nécessaire, les fichiers journaux peuvent être traités dans le cadre d'une enquête administrative, qu'il s'agisse d'une infraction pénale ou disciplinaire.

2.2.6. Transferts de données

Les articles 7, 8 et 9 du règlement (CE) n° 45/2001 énoncent une série d'obligations qui s'appliquent lorsque le responsable du traitement de données transfère des données à caractère personnel à des tiers. Les règles diffèrent selon que le transfert est destiné à i) des institutions ou organes communautaires (article 7), ii) des destinataires relevant de la directive 95/46/CE (article 8) ou iii) d'autres types de destinataires (article 9).

Les transferts de données qui ont lieu dans le cadre des activités de contrôle de l'Internet sont, notamment, les suivants: i) les transferts de données au DRH afin de lui permettre de décider d'ouvrir ou non une enquête; *ii)* les transferts à des enquêteurs internes et *iii)* les transferts à l'OLAF lorsqu'une enquête est ouverte et que les conditions nécessaires à une intervention de l'OLAF sont réunies.

Tous ces transferts ont lieu entre des institutions ou organes communautaires ou en leur sein. Par conséquent, l'article 7 du règlement s'applique. L'article 7 du règlement (CE) n° 45/2001 dispose que les données à caractère personnel doivent être transférées si elles sont nécessaires «*à l'exécution légitime de missions relevant de la compétence du destinataire*». Pour se conformer à cette disposition, le responsable de la sécurité des TI doit, lorsqu'il transfère des données à caractère personnel, s'assurer que: *i)* le destinataire a les compétences adéquates et que *ii)* le transfert est nécessaire.

Le CEPD considère qu'en cas de suspicion fondée qu'un usage de l'ICTI est contraire à la PSI, le transfert de données au DRH est conforme à l'article 7. Le DRH est compétent pour exécuter la tâche pour laquelle les données sont transférées, pour connaître les faits et évaluer la mesure dans laquelle ils constituent une suspicion solide d'un acte contraire à la PSI et au statut, justifiant une décision d'ouvrir une enquête administrative et une procédure disciplinaire. Il convient de veiller à ce que le transfert de ces informations repose sur une base solide, lorsque la suspicion a été confirmée par un deuxième rapport faisant suite au contrôle renforcé mené pendant deux ou quatre semaines (voir le point 2.2.4 «Contrôle des URL consultés» ci-dessus). En d'autres termes, le premier rapport ne doit contenir aucune donnée à caractère personnel identifiable, comme les identifiants des utilisateurs ou les adresses IP.

Le CEPD considère que les transferts de données aux enquêteurs internes *(ii)* et à l'OLAF *(iii)* aux fins susvisées sont conformes à ces exigences. Dans les deux cas, les destinataires sont compétents pour exécuter la tâche pour laquelle les données sont transférées. De même, dans les deux cas, les transferts de données sont nécessaires à l'exécution de la mission des destinataires.

2.2.7. Droit d'accès et de rectification

Conformément à l'article 13 du règlement (CE) n° 45/2001, la personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, 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. La PCI précise que les personnes ont un droit d'accès aux

données, mais elle ne fait pas mention du droit de rectification.

Le CEPD rappelle que le droit d'accès est obligatoire, sauf exception, et que la Cour a mis en place les procédures permettant de l'exercer. Le droit d'accès comprend, notamment, le droit d'être informé et d'obtenir une copie des données traitées relatives à une personne sous une forme intelligible. La Cour doit mettre en place les procédures adéquates afin de garantir aux utilisateurs la possibilité d'exercer leur droit d'accès.

Dans certains cas, le responsable du traitement des données, en l'occurrence la Cour des comptes, peut être en mesure d'invoquer l'une des exceptions visées à l'article 20, paragraphe 1, du règlement (CE) n° 45/2001 pour reporter l'octroi du droit d'accès ou de rectification. En l'espèce, ce report peut être légal, entre autres, lorsqu'une telle limitation constitue une mesure nécessaire pour «*(a) assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales*». Lorsqu'elle décide d'invoquer une exception, la Cour doit procéder à une évaluation au cas par cas des circonstances du traitement de données considéré.

Lorsque la Cour invoque une exception pour reporter l'octroi de l'accès, elle doit tenir compte du fait que les limitations d'un droit fondamental ne peuvent s'appliquer de manière systématique. La Cour doit, dans chaque cas, déterminer si les conditions d'application de l'une des exceptions sont réunies. En outre, comme le prévoit l'article 20 du règlement, la mesure doit être «nécessaire». Ce «critère de nécessité» doit être appliqué au cas par cas. Lorsque la Cour impose une exception, elle doit être conforme à l'article 20, paragraphe 3, selon lequel «*la personne concernée est informée conformément au droit communautaire des principales raisons qui motivent cette limitation et de son droit de saisir le contrôleur européen de la protection des données*». Cependant, la Cour peut se prévaloir de l'article 20, paragraphe 5, pour reporter la fourniture de cette information conformément à ladite disposition: «*L'information visée aux paragraphes 3 et 4 peut être reportée aussi longtemps qu'elle prive d'effet la limitation imposée sur la base du paragraphe 1*».

Conformément à l'article 14 du règlement (CE) n° 45/2001, la personne concernée a le droit de rectifier les données inexactes ou incomplètes. Étant donné la nature des données (fichiers journaux reliés à des identifiants d'utilisateurs et à des adresses IP) et la manière dont elles sont collectées (consignation automatique), la possibilité de rectification des données paraît extrêmement improbable. Par conséquent, il est également improbable que ce droit puisse être exercé. Cependant, en principe, la Cour doit reconnaître l'existence de ce droit, qui peut s'appliquer dans un nombre limité de cas, par exemple lorsqu'une personne utilise l'identifiant d'un autre utilisateur.

2.2.8. Information de la personne concernée

Conformément aux articles 11 et 12 du règlement (CE) n° 45/2001, les personnes qui collectent des données à caractère personnel sont tenues d'informer la personne que des données la concernant sont collectées et traitées. La personne concernée a également le droit d'être informée, notamment, des finalités du traitement, des destinataires des données et des droits spécifiques qu'elle possède en tant que personne concernée. La question de savoir si le canal de communication utilisé pour transmettre ces informations aux personnes concernées est adéquat est analysée ci-après. Des orientations sont également données sur le contenu des informations à fournir aux utilisateurs afin d'assurer la conformité avec le règlement (CE) n° 45/2001.

Le canal de communication. Selon la notification et les informations de suivi transmises par la Cour, afin de garantir le respect des articles 11 et 12, les utilisateurs de l'ICTI ont été officiellement informés de la procédure de contrôle par le biais d'une *annonce officielle* et de la publication de la PSI et de la FAQ sur l'Intranet de la Cour. La PCI sera prochainement rendue publique de la même

manière. En outre, lors de la première connexion à l'Internet, l'utilisateur doit confirmer qu'il a lu et compris la PSI. Enfin, les utilisateurs essayant d'accéder à un site Internet interdit sont informés du fait que l'accès a été refusé et des motifs du refus (le site Internet fait partie d'une catégorie indésirable, avec mention du nom de la catégorie). Le message invite l'utilisateur à prendre contact avec le service d'aide du responsable de la sécurité des TI pour un complément d'information.

Le CEPD souligne que la Cour doit faire en sorte que le canal choisi pour informer de l'existence du contrôle permette à chacun de prendre note efficacement de son contenu. Un contrôle caché, dont les utilisateurs ignorent l'existence, n'est pas admissible. En l'espèce, l'annonce officielle, la publication de la PSI sur l'Intranet, la PCI et la FAQ constituent une combinaison d'instruments adéquats pour informer les utilisateurs de l'existence de la procédure de contrôle. Le contenu de ces documents est relativement clair; les documents sont en permanence à la disposition des utilisateurs de l'ICTI pour consultation et, surtout, leur contenu est rappelé aux utilisateurs par des messages contextuels adressés aux personnes qui se voient refuser l'accès à certains sites Internet.

Une préoccupation soulevée par ces documents est le fait qu'ils fournissent les informations pertinentes de manière très dispersée. En effet, pour avoir accès aux informations juridiquement obligatoires, l'utilisateur de l'ICTI doit lire trois documents distincts: la PSI, la PCI et la FAQ. En outre, à première vue, le contenu et le rapport entre ces trois documents ne sont pas très clairs.

Il aurait été préférable de fournir les informations pertinentes, y compris le contenu des articles 11 et 12 du règlement (CE) n° 45/2001, dans un document unique plutôt que dans trois documents différents. Afin de réduire les conséquences d'une confusion éventuelle, le CEPD émet deux suggestions. Premièrement, une nouvelle FAQ pourrait être élaborée, souligner l'existence des deux documents de base (la PSI et la PCI) et clarifier le rapport entre ceux-ci. Deuxièmement, lorsque les utilisateurs se voient refuser l'accès à un site Internet, en même temps que les motifs du refus, un lien vers la PSI et la PCI pourrait s'afficher.

À titre supplémentaire et pour mieux faire connaître la PSI, le CEPD recommande également que la Cour procède à des audits périodiques des pratiques d'utilisation afin de déterminer si les procédures en vigueur sont bien comprises par les utilisateurs.

Le contenu de la politique. Le CEPD a examiné le contenu de la PSI, de la PCI et de la FAQ afin d'établir si ces documents contiennent les informations requises en application des articles 11 et 12 du règlement (CE) n° 45/2001. La combinaison de ces documents livre des informations sur la finalité du traitement, l'identité du responsable du traitement des données, l'existence du droit d'accès, les délais de conservation des données et le recours au CEPD. La PSI et la PCI font référence à la communication des données au directeur des ressources humaines. Le CEPD considère que cette information est conforme à l'article 11 du règlement (CE) n° 45/2001, à condition qu'il soit fait référence à la possibilité de transférer les données à l'OLAF, qui n'est actuellement mentionnée dans aucun des trois documents.

La description de ce qui constitue une utilisation abusive de l'Internet. Outre ce qui précède, il est essentiel que la déclaration relative à la vie privée contienne une définition claire de ce qui constitue une utilisation abusive de l'Internet. En particulier, les utilisateurs doivent connaître les paramètres qui seront contrôlés, par exemple, le volume téléchargé ou le temps passé sur la Toile. Par ailleurs, les utilisateurs doivent également être informés des types de sites jugés inadéquats, de sorte qu'ils sachent clairement ce qui est autorisé ou non.

Le CEPD observe que la description initiale de la manière dont le contrôle se déroule dans la PSI a été complétée par une liste de catégories de sites Internet dont l'accès est interdit. Cette liste apparaît dans la FAQ. Bien que la liste contienne quelques doubles emplois (les sites Internet sur la

nudité, le contenu destiné aux adultes et le sexe, semblent se rapporter au même type de contenu) et soit parfois vague (la définition de ce qui est considéré comme un site insipide n'est pas claire), dans un souci de transparence, l'établissement de cette liste est bienvenu.

2.2.9. Mesures de sécurité

Conformément aux articles 22 et 23 du règlement (CE) n° 45/2001, le responsable du traitement et le sous-traitant doivent mettre en oeuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et la nature des données à caractère personnel à protéger. Ces mesures de sécurité doivent, notamment, empêcher toute diffusion ou tout accès non autorisés, toute destruction accidentelle ou illicite, toute perte accidente ou toute altération, ainsi que toute autre forme de traitement illicite.

La division IT de la Cour confirme avoir pris les mesures de sécurité qu'impose l'article 22 du règlement et en a décrit certaines. Le CEPD n'a pas de raison de penser que ces mesures techniques et organisationnelles ne sont pas appropriées pour assurer un niveau de sécurité conforme aux risques présentés par le traitement et la nature des données à caractère personnel à protéger.

Le CEPD considère toutefois qu'étant donné que les historiques sont utilisés non seulement à des fins purement sécuritaires, mais aussi pour l'évaluation du comportement, les mesures de sécurité pourraient devoir être renforcées. Le CEPD recommande notamment les mesures suivantes: [....].

3. Conclusion

Les activités envisagées de traitement de données suscitent de sérieux doutes quant à leur compatibilité avec le règlement (CE) n° 45/2001, notamment en ce qui concerne leur nécessité et leur proportionnalité dans différents cas de figure. Afin d'assurer la conformité avec le règlement (CE) n° 45/2001, le CEPD recommande à la Cour des comptes:

1. de mettre tout en œuvre pour continuer à utiliser des techniques de filtrage qui suivent une approche préventive vis-à-vis de l'utilisation abusive de l'Internet plutôt qu'une approche répressive;
2. de reconsidérer la politique consistant à contrôler les URL des échecs de connexion à des sites Internet dont le contenu a été bloqué par des logiciels de filtrage ou d'autres techniques;
3. si le contrôle des échecs de connexion devait être jugé absolument nécessaire, de veiller à ce que les mesures de sauvegarde du traitement des données décrites dans le présent avis soient mises en œuvre lors du contrôle des URL de ces échecs et d'en informer le CEPD;
4. en l'absence de suspicion fondée, de s'abstenir de contrôler les URL des sites Internet consultés à moins que ce contrôle soit justifié, à savoir en cas de i) URL extrêmement longs et ii) de sites dangereux tels que ceux mentionnés par le SANS, le CERT et des publications similaires;
5. d'envisager l'utilisation d'autres indicateurs, tels que le volume des données téléchargées, pour découvrir les abus;
6. de s'assurer que les rapports mensuels communiqués au directeur des ressources humaines ne contiennent pas d'informations permettant d'identifier une personne (identifiant de l'utilisateur ou adresse IP);
7. de vérifier que les procédures appropriées existent pour donner aux utilisateurs la possibilité d'exercer leur droit d'accès et de rectification, sous réserve des exceptions pertinentes;
8. de modifier la FAQ et la PSI dans le sens suggéré par le présent avis;
9. de réaliser des audits périodiques des pratiques d'utilisation afin de vérifier que les

procédures de contrôle sont bien comprises par les utilisateurs;

10. d'introduire un lien vers la déclaration relative à la vie privée dans le message contextuel qui informe les utilisateurs que l'accès à un site Internet est bloqué;
11. de renforcer les mesures de sécurité relative aux fichiers journaux et d'assurer la conservation des documents susvisés.

Fait à Bruxelles, le 10 novembre 2008

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données