Avis sur la notification d'un contrôle préalable reçue du Délégué à la protection des données de la Commission européenne relatif à l'enregistrement de la ligne réservée aux appels relatifs aux urgences et à la sécurité à Bruxelles (n° 88888)

Bruxelles, le 22 mai 2006 (Dossier 2006-2)

1. Procédure

1.1. Le 3 janvier 2006, le Contrôleur Européen de la Protection des données (CEPD) a reçu une notification pour contrôle préalable en vertu de l'article 27 du Règlement (CE) 45/2001 (ci-après "le Règlement") du délégué à la protection des données de la Commission européenne (DPD). Cette notification concerne l'enregistrement des communications effectuées sur la ligne réservée aux urgences et à la sécurité à Bruxelles (n° 88888).

1.2. La notification est accompagnée d'un document intitulé "Projet de communication sur la création des offices - DG Admin" et d'une décision de la Commission (94) 2129 relative aux tâches du bureau de Sécurité.

1.3. Une demande d'informations supplémentaires a été formulée le 18 janvier 2006. Une réponse à cette demande a été donnée le 6 avril 2006.

2. Examen de l'affaire

2.1. Les faits

En cas d'urgence, le personnel de la Commission peut former le numéro d'appel d'urgence affiché dans tous les bâtiments de la Commission à Bruxelles à savoir le "88888".

Il ne peut être exclu que des personnes externes au personnel de la Commission utilisent le numéro d'urgence mis à disposition lorsqu'ils se trouvent dans une telle situation au sein de la Commission.

Dans le cadre des permanences de sécurité, la Direction Sécurité (DS) de la Direction générale Personnel et Administration procède à des enregistrements des appels reçus sur la ligne n° 88888 (appels d'urgence) à Bruxelles. Le système enregistre le contenu de la conversation téléphonique, l'heure de l'appel, la durée et le numéro où l'appel a abouti. Les personnes appelantes ne doivent pas nécessairement s'identifier au cours de la conversation. Le système utilisé ne permet pas de connaitre automatiquement les coordonnées de la personne qui a appelé les lignes concernées, ni de quel endroit l'appel provient sauf si ces informations sont données au cours de la conversation.

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.: 32-2-283 19 00 - Fax : 32-2-283 19 50

L'enregistrement a pour finalité la vérification *a posteriori* de la teneur des messages aboutissant sur les lignes concernées, la vérification a postériori des événements opérationnels et, dans le cadre de dossiers relatifs aux menaces pouvant peser sur l'institution, apporter les éléments de preuve.

Les appels sont enregistrés automatiquement sur support informatique. Ces enregistrements sont conservés trois mois à moins qu'elles n'entrent dans le cadre d'une procédure d'enquête officielle.

Les données sont destinées à un usage interne par le personnel statutaire autorisé de la Direction Sécurité. En effet, dans le cadre de la vérification des alertes et pour certains rapports d'enquête de la DS, les enregistrements sont écoutés et/ou utilisés par les trois personnes habilités à le faire, tous trois fonctionnaires responsables de service, habilités au secret et détenteurs des codes et des mots de passe nécessaires. Cette procédure est subordonnée aux instructions formelles et préalables du Chef de l'unité ADMIN.DS. 1. Le système enregistre toutes les requêtes d'écoute contenant la date, l'heure et les canaux écoutés. Le système conserve les enregistrements qui ont été écoutés.

Une transmission éventuelle aux autorités judiciaires nationales est possible selon les procédures légales en vigueur. Dans ce cas une trace en est conservée dans les archives du service.

Le personnel de surveillance est informé de l'enregistrement des appels et de l'usage qui en est fait lors de leur formation d'entrée en fonction. En outre, le fait que les lignes sont enregistrées est indiqué dans les consignes de la Permanence.

Selon les informations reçues par le DPD, actuellement sous couvert de l'exception de l'article 20 §1 sous a) du règlement 45/2001, aucune publicité a priori n'est donné du système d'enregistrement, de même que l'enregistrement de la communication n'est pas signifié à l'appelant. Toutefois, afin d'informer les personnes concernées à l'intérieur de la Commission, une déclaration de confidentialité a été préparée pour être incluse sur le site de la Direction Sécurité. Cette déclaration reprend l'identité du responsable du traitement, la finalité de la collecte, les personnes auxquelles les données sont éventuellement communiquées, le droit d'accès aux données des personnes concernées, la durée de conservation et les points de contact en cas de questions ou de plaintes.

En ce qui concerne les personnes extérieures, une mention spécifiant que les lignes sont enregistrées va être ajoutée à l'annuaire électronique disponible depuis l'extérieur de l'institution.

Il n'existe pas d'indexation des enregistrements à partir du nom des personnes impliquées. Toutefois, une personne qui le souhaite peut demander l'accès à l'enregistrement moyennant une vérification du bien fondée de la demande sur base de la date et de l'heure de l'appel.

Des mesures de sécurité ont été prises [...]

2.2. Les aspects légaux

2.2.1. Contrôle préalable

Le règlement 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. Il s'applique au traitement de données à caractère personnel par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire.

Nous sommes en présence ici d'un traitement par la Commission mis en œuvre dans le cadre d'activités communautaires. Par ailleurs il s'agit d'un traitement de données personnelles puisqu'il s'agit de l'enregistrement de communications entre deux personnes dont au moins l'une d'entre elle est identifiée ou au moins "identifiable". En effet, est réputée "identifiable" au sens de l'article 2 sous a) du règlement "une personne qui peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale". Puisque l'enregistrement mentionne le numéro où l'appel a abouti, il est possible, dans la plupart des cas, d'identifier la personne de service ce jour là. Par ailleurs, dans certains cas la personne ayant effectué l'appel s'identifie également.

Le règlement 45/2001 est dès lors applicable.

L'enregistrement est constitutif d'un traitement automatisé selon les termes du règlement.

L'article 27 §1 du règlement (CE) 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 §2 du règlement contient une liste des traitements susceptibles de présenter de tels risques.

Le traitement de données dans le cadre des réseaux internes de communication présente des aspects particuliers en matière de protection des données, qui ont conduit à la rédaction d'un chapitre spécialement dédié à ses aspects (Chapitre IV). Notamment l'article 36 prévoit le principe fondamental de la confidentialité des données qui sera examiné ci-après. Ce traitement particulier de telles données constitue un risque spécifique au sens de l'article 27 §1.

Par ailleurs, l'article 27 §2 sous a), prévoit que sont susceptibles de présenter des risques, les traitements de données relatifs à des suspicions, infractions, condamnations pénales ou mesures de sûreté. Puisque dans le cadre de dossiers relatifs aux menaces portant sur l'institution, ces enregistrements sont susceptibles d'apporter des éléments de preuve par rapport à des suspicions ou infractions, ils sont susceptibles de tomber sous le champ de l'article 27 §2. Enfin, des données relatives à la santé sont susceptibles d'être inclues dans la communication ce qui qualifie le traitement pour contrôle préalable également sous l'article 27 §2 sous a).

Pour ces raisons, le traitement doit faire l'objet d'un contrôle préalable.

En principe, le contrôle effectué par le Contrôleur européen de la protection des données est préalable à la mise en place du traitement. Dans ce cas, en raison de la nomination du Contrôleur européen à la protection des données, qui est postérieure à la mise en place du système, le contrôle devient par la force des choses a postériori. Ceci n'enlève rien à la mise en place souhaitable des recommandations présentées par le Contrôleur européen à la protection des données.

La notification du DPD a été reçue le 3 janvier 2006. Conformément à l'article 27 §4, le présent avis doit être rendu dans les deux mois qui suivent. Le délai pour rendre son avis a été suspendu pendant 77 jours par une demande d'informations complémentaires. Le contrôleur

rendra donc son avis au plus tard le 20 mai 2006. Puisque ce jour est un samedi, l'avis sera rendu le premier jour ouvrable qui suit, à savoir le 22 mai 2006.

2.2.2. Base légale et licéité du traitement

La Direction de la Sécurité assure la protection des personnes, des informations et des biens de la Commission (Charte du Bureau de Sécurité établie dans le document C(94)2129 du 8 septembre 1994). Dans ce contexte elle gère le service de permanence de la Commission où aboutissent les appels d'urgence. Dans le cadre de la mise en place de l'équipement de la Cellule Technique de Crise, dont fait partie la permanence de la sécurité, le Comité de Sécurité, présidé par le Secrétaire Général, a autorisé un système d'enregistrement permanent des communications destinées au Bureau de Sécurité et à la Cellule Technique en cas de crise (document CS/87/026 et 029). Ce document constitue la base légale.

L'analyse de la base légale s'accompagne de l'analyse de la licéité du traitement telle que définie à l'article 5 du règlement (CE) 45/2001. L'article 5 sous a) prévoit que le traitement de données à caractère personnel ne peut qu'être effectué si le traitement est "nécessaire à l'exécution d'une mission relevant 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". La base légale relevant des dispositions ci-dessus mentionnées, vient à l'appui de la licéité du traitement dans la mesure où l'enregistrement est nécessaire pour l'accomplissement des missions dévolues à la Direction Sécurité.

2.2.3. 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 bases soient trouvées au sein de l'articles 10 §2.

Des informations relatives à l'état de santé d'une personne peuvent figurer dans l'enregistrement d'appels d'urgence dans la mesure où certains appels portent précisément sur des appels pour urgence médicale. Dans la majorité des cas, la personne concernée aura donné son consentement au traitement de ses données justifiant par là le traitement sur base de l'article 10 §2 sous a). Enfin le traitement peut également se fonder sur l'article 10§2 sous c) lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

2.2.4. Qualité des données

En vertu de l'article 4 §1 sous c) du règlement "les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement". Par ailleurs elles doivent être "exactes et, si nécessaire, mises à jour" (article 4 §1 sous d).

Les données, objet du présent contrôle préalable concernent l'entièreté des conversations vers le numéro 88888 ainsi que l'heure, la durée de l'appel et le numéro où l'appel a abouti.

Il n'est pas souhaitable de procéder à une sélection des données au sein même de la conversation puisqu'à priori toutes les données sont pertinentes en vue des finalités poursuivies.

Par ailleurs les autres données de trafic sont également nécessaires pour les finalités du traitement.

L'enregistrement en direct des communications garanti l'exactitude des données.

Le CEPD considère dès lors que le principe de qualité des données est respecté.

2.2.5. Conservation des données

Le règlement prévoit que les données sont "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 §1 sous e).

La conservation des enregistrements pendant 3 mois est conforme à l'article 4 §1 sous e) du règlement.

Par ailleurs, en vertu de l'article 37 §1, les données de trafic, à savoir les données qui sont nécessaires afin d'établir les communications sont effacées ou rendues anonymes à la fin de la communication. Des exceptions à ce principe sont prévues par l'article 20 notamment lorsque cette exemption est nécessaire pour "assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales", "garantir la protection de la personne concernée" ou "assurer la sécurité nationale, la sécurité publique et la défense des Etats membres".

Les données relatives aux conversations téléphoniques sont conservées pendant 3 mois. Cette conservation des données, dont notamment des données de trafic, après la fin de la communication peut se fonder sur les exceptions prévues par l'article 20.

En cas de traitement de ces données nécessaires pour une enquête de sécurité/administrative, les données sont gardées jusqu'à aboutissement final de l'enquête et les possibles recours en justice. Cette période de conservation est également justifiée à la lumière des exceptions prévues à l'article 20.

2.2.6. Transfert des données

L'on ne peut exclure une communication éventuelle aux autorités nationales judiciaires selon les procédures légales en vigueur à des fins nationales propres. L'article 8 du règlement est applicable à tout transfert de données vers des destinataires autres que les institutions et organes communautaires et relevant de la Directive 95/46/EC. Il est vrai que la Directive 95/46/EC ne vise pas les activités judiciaires et l'article 8 du règlement n'est pas d'application *a priori*. Ceci étant dit, certains états membres ont étendu la portée de leur loi nationale transposant la directive afin d'y inclure les autorités nationales dans l'exercice de leur fonction judiciaire. Dans ces cas l'article 8 est d'application et le transfert ne peut que avoir lieu si le destinataire démontre que les données sont nécessaires à l'exercice d'une mission effectuée dans l'intérêt public ou relevant de l'autorité publique. Dans les autres cas, soit l'article 9 §1 est applicable pour les pays offrant un niveau de protection adéquate, soit l'article 9 §6 d) est applicable en vertu duquel le transfert est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêt public importants ou pour la constatation, l'exercice ou la défense d'un droit de justice.

2.2.7. Confidentialité des données

En vertu de l'article 36 du règlement, les institutions et organes communautaires garantissent la confidentialité des communications réalisées au moyen de réseaux de télécommunications et des équipements de terminaux dans le respect des principes généraux de droit communautaire.

Cette obligation de confidentialité s'applique au contenu même d'une communication. Il interdit, en principe, toute interception ou enregistrement des communications. Toute restriction à ce principe devra se faire dans le respect des principes généraux de droit communautaire. Ce dernier concept se réfère à la notion de droits fondamentaux, tels qu'établis par la Convention Européenne des Droits de l'Homme.

En pratique cela implique que toute restriction à la confidentialité des données doit se faire en respectant les droits fondamentaux tels qu'établis dans la Convention. Toute restriction ne peut être faite que si elle est prévue par la loi et si est nécessaire dans une société démocratique, notamment à des fins de sécurité nationale, sûreté publique, à la défense de l'ordre et à la prévention des infractions pénales ou à la protection des droits et libertés d'autrui.

Toute restriction au principe de confidentialité devra donc être examinée à la lumière de critères stricts et notamment de proportionnalité par rapport à des finalités précises.

Dans le cas présent, l'enregistrement des communications se faisant à des fins de sûreté publique, de défense de l'ordre ou à la prévention des infractions pénales, le CEPD estime qu'il n'y a pas de violation du principe de confidentialité pour autant que les données soient limitées à ce qui est strictement nécessaire.

2.2.8. Droit d'accès et de rectification

En vertu des articles 13 et 14 du règlement (CE) 45/2001, les personnes concernées disposent d'un droit d'accès et de rectification des données personnelles les concernant.

L'article 20 du règlement 45/2001 prévoit des restrictions au droit d'accès notamment si une telle mesure constitue une mesure nécessaire pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales. Cet article a été interprété par le CEPD comme permettant également des limitations dans le cadre d'enquêtes disciplinaires (voir l'avis 2004-0198). Il semble que l'usage de cette limitation pourrait être exercé dans certains cas en cas d'enquête sur base d'enregistrements de la Direction Sécurité. Le CEPD souhaite souligner qu'une telle restriction doit être limitée au temps nécessaire dans le cadre d'une enquête.

Le système permet l'accès des personnes concernées aux enregistrements les concernant. Une éventuelle rectification des données semble très rare car les enregistrements étant fait en direct, ils reflètent la réalité de l'appel.

2.2.9. Information des personnes concernées

En vertu de l'article 11 du règlement, tout traitement de données à caractère personnel implique que les personnes concernées soient suffisamment informées de ce traitement. Cette information doit normalement se faire au plus tard au moment de la collecte des données auprès de la personne concernée sauf si la personne concernée a déjà été informée. L'article 20 permet des exceptions à ce principe notamment lorsqu'une telle mesure constitue une

mesure nécessaire pour "assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales" (article 20 §1 sous a) ou afin d'assurer la sûreté nationale, la sécurité publique et la défense des Etats membres" (article 20 §1 sous d).

Selon les informations reçues par le DPD, actuellement sous couvert de l'exception de l'article 20 §1 sous a), aucune publicité a priori n'est donné du système d'enregistrement, de même que l'enregistrement de la communication n'est pas signifié à l'appelant. Le personnel de permanence du Bureau de sécurité est par contre informé de l'enregistrement des appels et de l'usage qui en est fait. Toutefois, un projet de déclaration de confidentialité qui serait inséré sur le site web de la Direction Sécurité informe les personnes concernées en interne à la Commission de l'enregistrement des données et reprend les rubriques de l'article 11 du règlement. Le CEPD soutient cette initiative.

Il ne peut être exclu que des personnes externes au personnel de la Commission utilisent les téléphones au sein de la Commission afin de former le numéro d'urgence. En ce qui concerne les personnes extérieures, une mention spécifiant que les lignes sont enregistrées va être ajoutée à l'annuaire électronique disponible depuis l'extérieur de l'institution. Toutefois, afin de respecter pleinement le règlement 45/2001, le CEPD recommande qu'au minimum un lien vers les autres rubriques de l'article 11 soit prévu.

2.2.10. Sécurité

L'article 22 du règlement prévoit que des mesures techniques et organisationnelles doivent être prises afin d'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.

Après une analyse attentive par le CEPD des mesures de sécurités adoptées, le CEPD considère que ces mesures sont adéquates à la lumière de l'article 22 du règlement (CE) 45/2001.

Conclusion

Le traitement proposé ne paraît pas entraîner de violations des dispositions du règlement (CE) 45/2001 pour autant qu'il soit tenu compte des observations faites ci-dessus. Cela implique, en particulier, que:

- Toute restriction au droit d'accès aux donnes doit être strictement limitée au temps nécessaire dans le cadre d'une enquête;

- le projet de déclaration de confidentialité qui va être inséré sur le site web de la Direction Sécurité informe effectivement les personnes concernées en interne à la Commission de l'enregistrement des données en reprenant les rubriques de l'article 11 du règlement;

- dans la mention spécifiant que les lignes sont enregistrées qui va être ajoutée à l'annuaire électronique disponible depuis l'extérieur de l'institution, il soit prévu au minimum un lien vers les autres rubriques de l'article 11.

Fait à Bruxelles, le 22 mai 2006.

J. BAYO DELGADO
Le Contrôleur adjoint européen de la protection des données

Note de suivi 24 août 2006

En date du 8 juin 2006, la Commission a pris en compte l'ensemble des recommandations figurant dans la conclusion de cet avis.

Le Contrôleur européen de la protection des données