

GIOVANNI BUTTARELLI
CONTROLEUR ADJOINT

M. Johan Van Damme
Délégué à la protection des données
Cour des comptes européenne
12, rue Alcide De Gasperi
1615 - Luxembourg
LUXEMBOURG

Bruxelles, le 20 décembre 2011
GB/UK/mch/ D(2011) 2328 C 2011-0989

Objet: Dossier n° 2011-989 relatif à la notification d'un contrôle préalable sur le système de vidéosurveillance à la Cour des comptes européenne (CCE)

Monsieur,

Nous avons examiné les documents que vous avez communiqués au Contrôleur européen de la protection des données (CEPD) le 28 octobre 2011 ainsi que le 7 novembre 2011 concernant la notification d'un contrôle préalable sur les traitements liés au système de vidéosurveillance de la Cour des comptes européenne (CCE), conformément à l'article 27 du règlement (CE) n° 45/2001 (le règlement).

Le CEPD a adopté en mars 2010 des lignes directrices en matière de vidéosurveillance¹ (ci-après, les «lignes directrices»), en demandant aux organes et institutions de l'UE de mettre leurs pratiques actuelles en conformité avec ces lignes directrices pour le 1^{er} janvier 2011. Dans le présent dossier, sur la base de la notification du 28 octobre 2011, le CEPD ne mettra en exergue que les pratiques de la CCE qui ne semblent pas conformes aux principes du règlement et aux lignes directrices, et limitera son analyse juridique à ces pratiques. Il est clair que toutes les recommandations pertinentes formulées dans les lignes directrices s'appliquent aux traitements mis en place dans le cadre du système de vidéosurveillance à la Cour des comptes européenne (CCE).

1. Nécessité d'un contrôle préalable

La section 4.3 des lignes directrices décrit les situations dans lesquelles le CEPD considère que la notification d'un contrôle préalable prévue à l'article 27 du règlement est nécessaire pour

¹http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_FR.pdf

aider l'institution concernée à instaurer des garanties supplémentaires de protection des données lorsque ses activités vont au-delà des traitements courants pour lesquels les lignes directrices fournissent déjà des garanties suffisantes. Les situations évoquées à la section 4.3 des lignes directrices portent notamment sur:

- la vidéosurveillance envisagée à des fins d'enquête;
- le contrôle des employés et le traitement de catégories spéciales de données;
- le contrôle de sites où les personnes s'attendent à un respect plus important de leur vie privée.

a) La vidéosurveillance envisagée à des fins d'enquête

La notification soumise (section 16 du formulaire de notification) semble suggérer que le traitement doit faire l'objet d'un contrôle préalable conformément à l'article 27, paragraphe 2, point a) («...traitements de données relatives à la santé et traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté...») et le rapport de contrôle du système de vidéosurveillance indique (section 20) que «[l]e CEPD a reçu une notification en vue d'un contrôle préalable en 2011, étant donné que des images sont susceptibles d'être utilisées ultérieurement au cours d'une enquête».

La politique de vidéosurveillance de la CCE, à la section 6.2, précise que «[l]a CCE utilise son système de vidéosurveillance aux seules fins de sécurité et de contrôle d'accès...»; la section 6.3 souligne explicitement que «[l]e système n'est utilisé à aucune autre fin» et stipule que «[l]e système n'est en aucun cas utilisé comme un outil d'enquête (à l'exception d'enquêtes sur des incidents physiques de sécurité tels que des vols ou un accès non autorisé). Dans des circonstances exceptionnelles seulement, les images peuvent être transférées à des organismes d'enquête dans le cadre d'enquêtes officielles en matière disciplinaire ou pénale». Ces circonstances exceptionnelles sont définies (à la section 7.4 de la politique de vidéosurveillance de la CCE) comme suit: «les services de police locaux peuvent se voir accorder un accès si ce dernier est nécessaire pour enquêter sur des infractions pénales ou engager des poursuites en la matière...». Selon l'analyse d'impact sur la vie privée (section 5.1), «[s]i une infraction pénale a été commise et que la preuve de l'infraction se trouve sur l'enregistrement ou qu'une personne est en mesure d'identifier les auteurs de ladite infraction, les images enregistrées pourraient être remises aux autorités de police nationales». Comme indiqué à la section 5.4 de l'analyse d'impact sur la vie privée, ce transfert doit être officiellement demandé par un procureur.

Comme indiqué à la section 5.8 des lignes directrices, il n'est pas exclu que dans des circonstances exceptionnelles, la technologie de vidéosurveillance puisse servir à des fins d'enquête sans lien direct avec un incident physique de sécurité. Une analyse au cas par cas est nécessaire pour déterminer si cette utilisation est permmissible et si elle nécessite des garanties supplémentaires qui ne sont pas prévues par les présentes lignes directrices et la politique relative à toute proposition de vidéosurveillance de ce type doit faire l'objet d'une analyse d'impact et d'un contrôle préalable par le CEPD. En revanche, comme indiqué également à la section 5.8 des lignes directrices, lorsqu'un système est mis en place à des fins typiques de sécurité, comme c'est le cas de la CCE, les enregistrements vidéo *peuvent* servir à enquêter sur les incidents physiques de sécurité, par exemple l'accès non autorisé aux locaux ou à des pièces protégées, le vol, le vandalisme, un incendie ou l'agression physique d'une personne. Outre la dissuasion et la prévention, les systèmes de vidéosurveillance sont presque toujours destinés à faciliter l'enquête après un incident de sécurité et à apporter des preuves permettant de poursuivre le coupable.

Pour autant que le système de vidéosurveillance de la CCE ne soit pas délibérément installé ou conçu à des fins d'enquêtes internes dépassant le cadre des incidents de sécurité tels que ceux décrits ci-dessus, il ne devrait pas – sur la base des informations communiquées dans la notification – faire l'objet d'un contrôle préalable ex-post compte tenu des finalités d'enquête poursuivies.

b) Le contrôle des employés et le traitement de catégories spéciales de données

Alors que le formulaire de notification ne mentionne en soi aucune de ces finalités, la politique de vidéosurveillance de la CCE, à la section 5, indique que «...des caméras sont également placées à l'entrée de la salle informatique, à l'intérieur de la salle informatique et dans la salle de sport», et pourraient, en principe, être utilisées pour contrôler le travail du personnel ou, en ce qui concerne la salle de sport, des données relatives à la santé.

Toutefois, la politique de vidéosurveillance de la CCE, à la section 6.3, mentionne explicitement que «[l]e système n'est utilisé à aucune autre fin, par exemple, il n'est pas utilisé pour contrôler le travail des employés ou leur assiduité» et la section 6.6 exclut la collecte de catégories spéciales de données. Cette position est également étayée par les raisons exposées dans les documents soumis avec la notification pour les deux caméras:

- selon la section 1.3.1. de l'analyse d'impact sur la vie privée et la section 4 du formulaire de notification, la caméra de vidéosurveillance installée dans la salle de sport permet de *«s'assurer que des personnes s'exerçant seules n'ont pas été victimes d'un accident ou d'un malaise»*. Il ressort du rapport de contrôle du système de vidéosurveillance (section 29), qui indique que *«[l']expérience a démontré qu'il était parfois possible de reconnaître des personnes se trouvant à une distance de six mètres de la caméra. Dans tous les autres cas, on constate la présence d'une personne dans la salle, mais sans qu'il soit possible de l'identifier»*, qu'il semblerait que la caméra installée dans la salle de sport soit inappropriée à une telle finalité;
- [...] la section 6.2 de la politique de vidéosurveillance de la CCE décrit le système de vidéosurveillance, entre autres, comme *«...faisant partie des mesures visant à renforcer les politiques de sécurité globales de la CCE»* qui *«...permet d'empêcher, de dissuader, et si nécessaire, d'enquêter sur un accès physique non autorisé, y compris un accès non autorisé à...des infrastructures informatiques...»* et *«...permet d'empêcher, de découvrir et d'enquêter sur le vol de matériel ou d'actifs détenus par la CCE»*.

Sur la base des informations fournies dans la notification telle qu'elle a été soumise, le système de vidéosurveillance de la CCE ne devrait donc pas faire l'objet d'un contrôle préalable ex-post eu égard au contrôle des employés et au traitement de catégories spéciales de données.

c) Le contrôle de sites où les personnes s'attendent à un respect plus important de leur vie privée

Aux termes des lignes directrices, section 6.8, «les endroits où les personnes s'attendent à un respect plus important de leur vie privée» comprennent généralement des bureaux individuels, des endroits de détente, des sanitaires, des salles de douche et des vestiaires. Dans ce contexte, il convient de noter que les «endroits de détente» comprennent des équipements sportifs qui n'ont rien à voir avec la mission de l'institution, comme la salle de sport de la CCE². Il est indiqué à la section 6.8 des lignes directrices que les sites où les personnes s'attendent à un respect plus important de leur vie privée ne doivent pas faire l'objet d'une surveillance, qu'une

² La version actualisée de la politique de vidéosurveillance de la CCE (soumise le 7 novembre 2011) à la section 5 est conforme à la présente évaluation.

analyse d'impact doit être réalisée dans les cas où l'institution concernée souhaite déroger à ces règles et qu'un contrôle préalable par le CEPD est également requis.

Les traitements examinés sont donc soumis à un contrôle préalable ex-post, conformément à l'article 27 du règlement. Toutefois, ainsi que le CEPD l'a souligné lors de la publication des lignes directrices³, ce n'est que dans des cas exceptionnels que le contrôle préalable est exhaustif et qu'il couvre *tous* les aspects d'un système de vidéosurveillance. Dans la plupart des cas, le CEPD n'examine *pas* de manière exhaustive toutes les pratiques de l'institution en matière de vidéosurveillance.

Au lieu de cela, comme c'est le cas en l'occurrence, le CEPD concentre généralement ses recommandations sur les aspects de vidéosurveillance qui s'écartent des pratiques classiques et garanties standard exposées dans les lignes directrices ou qui viennent s'y ajouter (ici la vidéosurveillance de la salle de sport comme contrôle d'un site où les personnes s'attendent à un respect plus important de leur vie privée).

2. Procédure

La procédure a été notifiée le 26 octobre 2011 en vue du contrôle préalable prévu à l'article 27 du règlement (CE) n° 45/2001. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois. Au total, la procédure a été suspendue pendant 7 jours (par courrier électronique du 31 octobre 2011, jusqu'à réception, le 7 novembre 2011, d'annexes supplémentaires venant compléter la notification) et 4 jours pour permettre au DPD de soumettre ses observations. Par conséquent, le présent avis doit être rendu au plus tard le 9 janvier 2012.

3. Salle de sport: contrôle d'un site où les personnes s'attendent à un respect plus important de leur vie privée

Faits: comme indiqué ci-dessus, la salle de sport de la CCE est un «endroit de détente» au sens de la section 6.8 des lignes directrices et de ce fait un site où les personnes s'attendent à un respect plus important de leur vie privée qui ne devrait pas, en principe, faire l'objet d'une surveillance comme le prévoient les lignes directrices.

- Selon la section 1.3.1. de l'analyse d'impact sur la vie privée et la section 4 du formulaire de notification, la caméra de vidéosurveillance installée dans la salle de sport permet de *«s'assurer que des personnes s'exerçant seules n'ont pas été victimes d'un accident ou d'un malaise»*.
- L'analyse d'impact sur la vie privée (sections 6.3 et 1.10 respectivement) mentionne également à cet égard que *«[l]e seul risque identifié pour la vie privée est le fait que les images enregistrées par la caméra installée dans la salle de sport, qui permet d'identifier les personnes s'exerçant à une distance de 5 mètres de la caméra, pourraient être utilisées pour espionner ces sportifs. La direction générale a estimé que ce risque était acceptable.»* et que *«[l]e comité du personnel a posé des questions quant à l'intérêt de cette caméra et si la présence à plein temps d'un entraîneur sportif/garde de sécurité ne serait pas une meilleure alternative»*.
- [...]

³ Voir «Frequently asked questions on video-surveillance: prior checking» (Foire aux questions sur la vidéosurveillance: contrôle préalable), section 5, disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_FAQ_videosurveillance_EN.pdf

Recommandation:

Du point de vue du respect de la vie privée dès la conception et comme indiqué à la section 6.4 des lignes directrices, «...[l]orsque l'identification n'est pas nécessaire par contre, la résolution des caméras et les autres paramètres modifiables doivent être choisis de façon à ne pas enregistrer d'images faciales reconnaissables». Afin que le personnel de sécurité puisse porter secours aux personnes victimes d'un accident ou d'un malaise dans la salle de sport, il n'est pas nécessaire de reconnaître les personnes à une distance de six mètres de la caméra. La CCE devrait donc s'assurer, sur le plan technique, que dans tous les cas on puisse constater la présence d'une personne dans la salle, mais sans qu'il soit possible de l'identifier. Faute d'informations supplémentaires, le CEPD n'est pas en mesure d'apprécier les implications en matière de sécurité de la présence à plein temps d'un entraîneur sportif/garde de sécurité et de son efficacité par rapport au système de vidéosurveillance en l'occurrence. Cependant, du point de vue de la protection des données, il semblerait que la surveillance/reconnaissance directe par un entraîneur sportif/garde de sécurité présent sur place soit moins respectueuse de la vie privée qu'un système de vidéosurveillance sans possibilités d'identification, tel que recommandé.

4. Rappels concernant d'autres aspects de la politique de vidéosurveillance de la CCE

a) Période de conservation

Selon la section 8 de la politique de vidéosurveillance de la CCE, la période de conservation normale pour les séquences des bâtiments K1 et K2 est de 16 jours. Elle est donc plus longue que celle recommandée à la section 7.1 des lignes directrices. Selon le rapport de contrôle du système de vidéosurveillance, «[c]ette période est justifiée par le fait que la CCE ferme complètement entre Noël et Nouvel an et que le personnel chargé de la sécurité physique n'est pas disponible. Pour permettre à ces personnes d'enquêter sur un incident physique de sécurité, les images doivent être conservées pendant la période maximale durant laquelle la CCE est fermée, plus cinq jours ouvrables pour chercher les images, les copier et/ou les transférer».

Comme le CEPD l'a précisé précédemment⁴, si les institutions ne fournissent pas de justification suffisante et de garanties adéquates, elles doivent réduire la période de conservation à sept jours ou moins, conformément aux recommandations des lignes directrices. Il semblerait que d'autres organes aient trouvé des solutions techniques pour couvrir la période entre Noël et Nouvel an. En tout état de cause, des spécificités concernant un événement qui n'a lieu qu'une fois dans l'année peuvent difficilement justifier une période de conservation *standard*. Le CEPD a donc invité la CCE à reconsidérer la période de conservation actuelle de 16 jours.

[...]

c) Avis affiché sur place et version publique de la politique de vidéosurveillance de la CCE

La section 5.1.2 des lignes directrices prévoit que l'objectif du système doit être communiqué au public sous une forme sommaire à l'endroit concerné, et sous une forme plus détaillée, par exemple, via une version publique en ligne de la politique de vidéosurveillance de l'institution.

- Comme indiqué dans le rapport de contrôle du système de vidéosurveillance (observations 10, 24, 27): la CCE devrait s'assurer de la transparence de sa politique

⁴http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-14_Videosurveillance_followup_EN.pdf

de vidéosurveillance et de la notice de synthèse figurant sur les pages intranet et internet dédiées (les liens vers la politique de vidéosurveillance et la notice de synthèse devraient renvoyer à ces documents).

- L'avis affiché sur place mentionné à la section 9.1 de la politique de vidéosurveillance de la CCE ne satisfait pas à toutes les exigences de contenu visées à la section 11.2 des lignes directrices. La CCE devrait revoir l'avis de manière à ce qu'il établisse un lien vers la politique de vidéosurveillance mise en ligne (les liens devraient renvoyer à la politique de vidéosurveillance). Comme indiqué dans le rapport de contrôle du système de vidéosurveillance (observations 25 + 26) et la politique de vidéosurveillance de la CCE (section 9.1), un avis sur place doit être «affiché à proximité des sites surveillés». Alors qu'à la section 11.2 des lignes directrices, il n'est pas obligatoire d'afficher un avis à côté de chaque caméra, le CEPD invite la CCE à s'assurer que les avis sont placés au bon endroit et qu'ils sont d'une taille suffisante, de sorte que les personnes concernées les remarqueront avant d'entrer dans une zone contrôlée et qu'ils les liront sans difficulté.

5. Conclusions

Le CEPD invite la CCE à adopter des mesures spécifiques et concrètes pour mettre en œuvre la recommandation précitée concernant la vidéosurveillance dans la salle de sport de la CCE.

Pour ce qui est des rappels mentionnés dans la présente note, le CEPD souhaite être informé de la situation concernant le respect des lignes directrices et recevoir les informations demandées.

Afin de faciliter notre suivi, nous vous saurions gré de bien vouloir transmettre au CEPD, dans un délai de trois mois à compter de la date de la présente, tous les documents pertinents prouvant que l'ensemble des recommandations et rappels ont été mis en œuvre.

Veillez croire, Monsieur, à l'assurance de ma considération distinguée,

(signé)

Giovanni BUTTARELLI