COUR DES COMPTES EUROPÉENNE
Secrétariat général

Cour des comptes européenne

Sécurité de l'information

Brochure sur la politique en matière de vidéosurveillance

1. INTRODUCTION

La Cour des comptes européenne (ci-après la "CdCE") utilise un système de vidéosurveillance afin d'assurer la sécurité de ses bâtiments, de ses biens, de son personnel et de ses visiteurs. L'intégralité de la politique en matière de vidéosurveillance est disponible à l'adresse eca.europa.eu/CCTV.

2. GARANTIE D'UNE UTILISATION EFFICACE ET CIBLÉE DE LA VIDÉOSURVEILLANCE

2.1. Révision du système existant

Le système de vidéosurveillance est conforme aux lignes directrices en matière de vidéosurveillance publiées par le Contrôleur européen de la protection des données (ci-après «lignes directrices») le 17 mars 2010.

L'autorité de protection des données compétente au Luxembourg, la CNPD, a été informée. Par ailleurs, l'avis affiché sur place et la présente politique de vidéosurveillance sont également disponibles en anglais et en allemand.

2.2. Solutions technologiques respectueuses de la vie privée

Les solutions suivantes, respectueuses de la vie privée, ont été déployées (voir chapitre 3.4 des lignes directrices):

- caméras basse résolution,
- technologie image par image.

3. ENDROITS SOUS SURVEILLANCE

Les caméras sont situées aux entrées et sorties des bâtiments, ainsi qu'à l'intérieur de la salle informatique et de la salle de fitness.

Il n'y a pas d'autre caméra ailleurs, que ce soit à l'intérieur ou à l'extérieur des bâtiments. Sauf dans la salle de fitness[1], aucune surveillance n'est exercée dans les endroits où les personnes peuvent s'attendre à un respect accru de leur vie privée, par exemple les bureaux individuels, les espaces de détente, les locaux sanitaires, etc. (voir chapitre 6.8 des lignes directrices). L'emplacement des caméras a été choisi avec soin de façon à limiter le plus possible la surveillance de zones ne présentant aucun intérêt au regard de l'objectif fixé (voir chapitre 6.1 des lignes directrices).

Il n'y a pas de surveillance à l'extérieur des bâtiments de la CdCE sur le territoire du Luxembourg, comme cela est recommandé au chapitre 6.5 des lignes directrices.

[1] Une caméra a été installée dans la salle de fitness pour le cas où un utilisateur isolé serait victime d'un accident ou d'un malaise.

4. COLLECTE DES INFORMATIONS PERSONNELLES ET FINALITÉ

Le système de vidéosurveillance est un système statique traditionnel. Il effectue un enregistrement numérique image par image. Il enregistre les images prises par les caméras dans chaque zone surveillée ainsi que l'heure, la date et l'endroit. Toutes les caméras fonctionnent 24 heures sur 24, 7 jours sur 7. La qualité des images permet parfois d'identifier les personnes se trouvant dans le champ des caméras (voir chapitre 6.4 des lignes directrices). Il n'est pas fait usage d'équipements de vidéosurveillance de haute technologie ou de vidéosurveillance intelligente (voir chapitre 6.9 des lignes directrices), le système n'est pas interconnecté avec d'autres systèmes (chapitre 6.10), et il n'y a ni surveillance dissimulée (chapitre 6.11), ni enregistrements sonores ou «caméras de surveillance parlantes» (chapitre 6.12).

La CdCE utilise son système de vidéosurveillance exclusivement à des fins de sécurité et de contrôle des accès.

Le système n'est utilisé à aucune autre fin. Il ne sert pas non plus d'outil d'investigation (hormis pour enquêter sur les incidents de sécurité physique tels que les vols et les accès non autorisés). Les images peuvent être communiquées aux organes d'investigation dans des circonstances exceptionnelles uniquement, en rapport avec une enquête criminelle ou disciplinaire formelle, comme celles décrites au point 7.4 (voir chapitres 5.7, 5.8 et 10.3 des lignes directrices).

La CdCE n'envisage aucune opération de surveillance *ad hoc* nécessitant une planification préalable à ce stade (voir chapitre 3.5 des lignes directrices).

Aucune webcam n'est installée à des fins de vidéosurveillance (voir chapitre 5.10 des lignes directrices).

Aucune donnée relevant de catégories spéciales n'est collectée (voir chapitre 6.7 des lignes directrices).

5. ACCÈS AUX DONNÉES ET DIVULGATION DE CELLES-CI

5.1. Personnel de sécurité interne

Seuls les membres du personnel responsables de la sécurité physique ont accès aux images enregistrées. La vidéo en temps réel est également accessible aux agents de sécurité.

5.2. Formation à la protection des données

Tous les membres du personnel possédant un droit d'accès aux images de vidéosurveillance ont reçu une formation de base à la protection des données.

5.3. Transferts et divulgations

Tous les transferts et toutes les divulgations en dehors de l'unité de sécurité doivent être documentés. Leur nécessité et la compatibilité de leur objectif avec la finalité première du système, à savoir la sécurité et le contrôle des accès, font l'objet d'une évaluation rigoureuse (voir chapitre 10 des lignes directrices). Un registre des séquences conservées et des transferts est joint en annexe 6 (voir chapitres 10.5 et 7.2 des lignes directrices). Au 28 octobre 2011, aucune entrée ne figurait dans le

registre en question. Le délégué à la protection des données est systématiquement consulté. Aucun accès n'est donné au personnel d'encadrement ou à la direction des ressources humaines.

5.4. Comment les informations sont-elles protégées et sauvegardées?

Un certain nombre de mesures techniques et organisationnelles ont été prises afin de garantir la sécurité du système de vidéosurveillance, y compris les données personnelles.

6. PÉRIODE DE CONSERVATION DES INFORMATIONS

Les images sont conservées pendant 16 jours au maximum (7 jours au bâtiment K8). Toutes les images sont ensuite physiquement écrasées par les nouvelles images enregistrées. Certaines images peuvent être gardées plus longtemps si leur conservation est nécessaire dans le cadre d'une enquête ou pour servir de preuve après un incident de sécurité. Cette conservation est rigoureusement documentée et sa nécessité est réévaluée régulièrement. Toute conservation doit être notifiée au délégué à la protection des données, qui détient le registre de conservation et des transferts (voir chapitre 7 des lignes directrices).

7. INFORMATIONS COMMUNIQUÉES AU PUBLIC

7.1. Notification individuelle spécifique

Les personnes identifiées sur caméra (par exemple, par le personnel de sécurité dans le cadre d'une enquête de sécurité) doivent par ailleurs en être informées à titre individuel si au moins l'une des conditions suivantes est remplie:

leur identité a été notée dans un dossier/un enregistrement,

l'enregistrement vidéo est utilisé à l'encontre de la personne,

l'enregistrement est conservé au-delà de la période de conservation normale,

l'enregistrement est transféré en dehors de l'unité de sécurité,

l'identité de la personne est communiquée à une personne extérieure à l'unité de sécurité.

Le cas échéant, le délégué à la protection des données est systématiquement consulté afin de garantir le respect des droits de la personne concernée.

8. VÉRIFICATION, CORRECTION ET SUPPRESSION D'INFORMATIONS

Les membres du public ont le droit d'accéder aux données personnelles les concernant détenues par la CdCE. Toute demande d'accès à des données à caractère personnel, ou de rectification, blocage et/ou suppression de celles-ci doit être adressée au responsable de la sécurité physique (ECA-Security@eca.europa.eu; tél. +352 4398-45911). Le délégué à la protection des données (ECA-Data-Protection@eca.europa.eu, tél. +352 4398-47777) peut également être contacté pour toute autre question relative au traitement de données à caractère personnel.

9. DROIT DE RECOURS

Toute personne a le droit de saisir le contrôleur européen de la protection des données (edps@edps.europa.eu) si elle considère que ses droits garantis par le règlement (CE) n° 45/2001 ont été violés du fait du traitement de ses données personnelles par la CdCE. Avant d'en arriver là, la CdCE recommande aux personnes concernées de prendre d'abord contact avec:

- le responsable de la sécurité (voir ci-dessus ses coordonnées) et/ou
- le délégué à la protection des données **(**ECA-Data-Protection@eca.europa.eu, tél. +352 4398-47777).

10. RÉFÉRENCES

Règlement (CE) n° 45/2001

Lignes directrices du CEPD en matière de vidéosurveillance