Notice informative relative à la vidéosurveillance dans les bâtiments de la Cour de justice de l'Union européenne

La présente notice fournit des informations relatives au système de vidéosurveillance générale mis en place par l'institution (1) ainsi que des informations concernant la possibilité de recourir à un dispositif ad hoc (2).

1) Informations relatives à la vidéosurveillance générale

L'institution a mis en place un système de vidéosurveillance pour assurer la sécurité générale des personnes et des biens conformément au Schéma directeur de mise en sûreté du complexe immobilier de la Cour de justice de l'Union européenne. Les finalités et les modalités du traitement des images filmées sont détaillées dans un document intitulé « Politique de vidéosurveillance » accessible sur le site internet de l'institution ainsi que sur les sites intranet de la Section sécurité et sûreté et du délégué à la protection des données.

Des caméras de surveillance sont placées tant à l'extérieur qu'à l'intérieur des bâtiments de l'institution (sélection aléatoire ou commandée des lieux filmés).

Les images des personnes concernées (personne accédant aux bâtiments de l'institution ou se trouvant aux abords extérieurs desdits bâtiments) sont les seules données collectées par le système.

La personne responsable du traitement des données est le Chef du Service de sécurité, tel +352 4303-1, securite@curia.europa.eu.

Les images sont enregistrées et utilisées conformément :

- au règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à 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,
- aux recommandations du Contrôleur européen de la protection des données (« CEPD ») reprises dans les lignes directrices en matière de vidéo surveillance du 17 mars 2010[1].

[1] Les lignes directrices en matière de vidéosurveillance sont disponibles sur le site internet du CEPD : https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Supervision/Guidelines

Les images sont traitées pour les finalités suivantes :

- Contrôles d’accès et de sécurité (sécurité des personnes, des bâtiments, des biens et des informations) ;
- Localisation d’un départ de feu, estimation d'impact pour une éventuelle évacuation d’un bâtiment, surveillance des issues de secours ;
- Surveillance des œuvres d'art ;
- Dissuasion (dégradations des biens de l'institution, atteintes aux personnes) ;
- Recherche des auteurs d'éventuelles infractions.

Les images enregistrées sont conservées pendant une durée maximale de 30 jours, mais, en cas de suspicion et/ou de constatation d’infraction, les données pertinentes sont conservées pendant la durée de l’enquête et de la procédure (par ex. disciplinaire ou pénale) qui éventuellement en découle. Les images enregistrées ne sont accessibles qu'à un nombre limité de personnes et toutes les mesures techniques et physiques sont mises en œuvre afin d'en éviter une utilisation inadéquate.

Les personnes suivantes ont accès aux images :

- Fonctionnaires et agents du Service de sécurité de la Direction des bâtiments (visualisation, enregistrement, copie, archivage, effacement) ;
- Agents de la société de gardiennage qui assurent partiellement les fonctions de sécurité (visualisation en temps réel sans accès aux images enregistrées).

Les images peuvent être communiquées à d'autres destinataires dans des cas particuliers :

- la Cour de justice (« Cour »), le Tribunal de l’Union européenne (« Tribunal ») et/ou le Tribunal de la fonction publique (« TFP »), ou un juge national, ainsi que les avocats et agents des parties dans l'hypothèse d'un litige ;
- l’instance de la Cour, du Tribunal, ou du TFP chargée d'examiner les réclamations, le Président et le Greffier de la juridiction concernée, ainsi que le conseiller juridique pour les affaires administratives, en cas de réclamation introduite en application de l'article 90, paragraphe 2, du statut des fonctionnaires ;
- les personnes appelées à exercer des fonctions dans le cadre d’une enquête administrative ordonnée par l’autorité investie du pouvoir de nomination ou l’autorité habilitée à conclure les contrats d’engagements ou dans le cadre d’une procédure disciplinaire, ouverte, selon les règles définies à l’annexe IX du statut des fonctionnaires de l’UE, à la suite d’un incident de sécurité ;
- le Président et le Greffier de la Cour, ainsi que des fonctionnaires qui les assistent, dans le cadre des responsabilités qui leur sont dévolues par l'article 20, paragraphe 4, du règlement de procédure de la Cour ;
- le CEPD conformément à l'article 47, paragraphe 2, du règlement n° 45/2001 ;
- le délégué à la protection des données de l'institution conformément au point 4 de l'annexe au règlement n° 45/2001 ;
- le Médiateur européen dans la mesure nécessaire au traitement d'une plainte auprès de lui (article 228 TFUE) ;
- l’OLAF en cas d'enquête effectuée en application du règlement n° 883/2013 et de la décision de la Cour de justice du 12 juillet 2011 relative aux conditions et modalités des

enquêtes internes en matière de lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts de l'Union européenne.

Enfin, dans les conditions définies par l'article 8 du règlement n° 45/2001, les images peuvent être transmises aux autorités nationales si cela s'avère nécessaire aux fins d'une enquête menée dans l'exercice de ses compétences.

Tous les transferts de données effectués sont consignés dans un registre spécifique.

Toute personne qui souhaite obtenir des informations supplémentaires ou exercer les droits qu'elle tire du règlement n° 45/2001 (accès, rectification, verrouillage, effacement ou opposition) peut s'adresser au Chef du Service de sécurité.

Les articles 13 et 14 du règlement n° 45/2001, relatifs, respectivement, au droit d'accès et au droit de rectification, sont cités *in extenso* ci-après.

La personne dont les données personnelles sont traitées a aussi la possibilité de saisir le CEPD au titre de l'article 32, paragraphe 2, du règlement n° 45/2001.

Article 13 du règlement n° 45/2001

Droit d'accès

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 :
a) la confirmation que des données la concernant sont ou ne sont pas traitées;
b) des informations au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées;
c) 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;
d) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant.

Article 14 du règlement n° 45/2001

Rectification

La personne concernée a le droit d'obtenir du responsable du traitement la rectification sans délai de données à caractère personnel inexactes ou incomplètes.

2) Informations relatives à la vidéosurveillance dissimulée (chapitre 4.4 de la politique de vidéosurveillance de la Cour de justice de l'Union européenne, « vidéosurveillance dissimulée »)

Le système de vidéosurveillance générale ne comprend aucun dispositif de vidéosurveillance dissimulée.

Dans le cadre d'une investigation interne de sécurité, sur base d'une analyse d'impact (soumise pour avis au délégué à la protection des données) et après décision du Greffier de la Cour, l'institution peut à titre exceptionnel avoir recours à un système de vidéosurveillance dissimulée, distinct et déconnecté du système de vidéosurveillance générale, pour rechercher des auteurs d'intrusions répétées, de vols ou d'autres infractions graves aux règles de sécurité.

L'analyse d'impact doit permettre de démontrer en quoi l'atteinte à la vie privée et à la protection des données à caractère personnel résultant de l'utilisation d'un système de vidéosurveillance dissimulée est compensée par les avantages tirés de l'utilisation dudit système.
À cette fin, cette analyse prend en compte, en sus des garanties qui encadrent l'utilisation de la vidéosurveillance générale, un ensemble de critères, parmi lesquels figurent l'absence de mesures alternatives plus respectueuses de la vie privée ainsi que les limites appliquées à l'emploi des équipements envisagés (lieu, horaires et délai de recours aux équipements, dont le choix est lui-même déterminé en fonction des infractions constatées).

Les équipements de vidéosurveillance dissimulée ne peuvent en aucun cas être connectés au système de vidéosurveillance générale. De ce fait, les images enregistrées sont relevées manuellement.
Ces images sont visionnées dès que possible et au plus tard endéans sept jours ouvrables suivant leur enregistrement afin d'en évaluer la pertinence. Cette durée maximale de sept jours ouvrables est nécessaire dans la mesure où des interventions quotidiennes sur les équipements pourraient nuire au bon déroulement de l'investigation interne de sécurité, mais aussi afin de disposer de suffisamment de temps pour procéder au relevé manuel des images sur lesdits équipements.

Les images qui ne sont pas pertinentes aux fins de l'investigation interne de sécurité sont effacées immédiatement après leur premier visionnage.
Les images pertinentes aux fins de l'investigation interne de sécurité sont conservées jusqu'à la clôture de cette investigation et des procédures faisant éventuellement suite à celle-ci.

Les personnes identifiées sur les images sont informées à titre individuel par la Section sécurité et sûreté si au moins l'une des conditions suivantes est remplie :

- l'identité de la personne a été notée dans un dossier;
- l'enregistrement vidéo est utilisé à l'encontre de la personne;
- l'enregistrement vidéo est conservé au-delà des délais prévus ci-dessus;
- l'enregistrement vidéo est transféré à l'extérieur de la Section sécurité et sûreté ou
- l'identité de la personne est communiquée à une personne extérieure à la Section sécurité et sûreté.

Cette information peut être retardée si cela est nécessaire aux fins de l'investigation interne de sécurité ou dans d'autres cas prévus par l'article 20 du règlement n° 45/2001 (cité *in extenso* ci-après).

Article 20 du règlement n° 45/2001

Exceptions et limitations

1. Les institutions et organes communautaires peuvent limiter l'application de l'article 4, paragraphe 1, de l'article 11, de l'article 12, paragraphe 1, des articles 13 à 17 et de l'article 37, paragraphe 1, pour autant qu'une telle limitation constitue une mesure nécessaire pour:

a) assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales;

b) sauvegarder un intérêt économique ou financier important d'un État membre ou des Communautés européennes, y compris dans les domaines monétaire, budgétaire et fiscal;

c) garantir la protection de la personne concernée ou des droits et libertés d'autrui;

d) assurer la sûreté nationale, la sécurité publique et la défense des États membres;

e) assurer une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) et b).

2. Les articles 13 à 16 ne s'appliquent pas lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle qui est nécessaire à seule fin d'établir des statistiques, sous réserve qu'il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée et que le responsable du traitement offre des garanties juridiques appropriées, qui excluent notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes déterminées.

3. Si une limitation prévue au paragraphe 1 est imposée, 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.

4. Si une limitation prévue au paragraphe 1 est invoquée pour refuser l'accès à la personne concernée, le contrôleur européen de la protection des données lui fait uniquement savoir, lorsqu'il examine la réclamation, si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées.

5. 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.