To be filled out in the EDPS' office

NUMERO DE REGISTRE: 1242

NOTIFICATION DE CONTRÔLE PREALABLE

Date de soumission :18/06/2014

Numéro de dossier : 2014-0598

Institution : COUR DE JUSTICE DE L'UNION EUROPEENNE

Base légale : article 27-5 du Règlement CE 45/2001du 18 décembre 2000 (1)

(1) Journal officiel de l'Union européenne L 8, 12.01.2001

INFORMATIONS NECESSAIRES (2)

(2) Merci de joindre tout document utile

1/ Nom et adresse du responsable du traitement

Chef de la Section sécurité et sûreté

Cour de justice de l'Union européenne

L-2925 Luxembourg

2/ Services de l'institution ou de l'organe chargés du traitement de données à caractère personnel

Section sécurité et sûreté de la Direction des Bâtiments.

3/ Intitulé du traitement

Vidéosurveillance dissimulée dans les bâtiments de la Cour de justice de l'Union européenne.

4/ Finalités du traitement

Dans le cadre d'une investigation interne de sécurité, sur base d'une analyse d'impact et après décision du Greffier de la Cour de justice de l'Union européenne, l'Institution peut 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.

Les caméras de surveillance dissimulées ne seraient placées que pour une période strictement limitée et dans des endroits bien précis en fonction des besoins de l'investigation interne de sécurité.

5/ Description de la catégorie ou des catégories de personnes concernées

Toute personne accédant aux bâtiments de la Cour de justice de l'Union européenne et se rendant dans les endroits faisant l'objet d'une vidéosurveillance dissimulée.

6/ Description des données ou des catégories de données ***(en incluant, si nécessaire, les catégories particulières de données (article 10) et/ou l'origine des données)***

Images filmées par des caméras dissimulées placées à l'intérieur des bâtiments de la Cour de justice de l'Union européenne.

La vidéosurveillance dissimulée exclut tout enregistrement sonore.

7/ Informations destinées aux personnes concernées

Les systèmes de vidéosurveillance dissimulée sont par nature installés de manière à ce que les personnes susceptibles d'être filmées ne soient pas informées de la présence de caméras dans les endroits où celles-ci sont placées.

L'information des personnes concernées au titre de l'article 12 du règlement n° 45/2001 fait donc l'objet d'une limitation au titre de l'article 20, paragraphe 1, sous a), du règlement n° 45/2001.

Cependant, la politique de vidéosurveillance qui est accessible sur le site intranet de la Section sécurité et sûreté (http://intranet/infrastructures/indispensables/securite.htm) et sur le site internet de l'institution (http://curia.europa.eu/jcms/jcms/P_127468) signale la possibilité pour la Cour, dans des rares cas, de mettre en place un système de vidéosurveillance dissimulée dans le cadre d'une investigation interne de sécurité pour une période strictement limitée et dans des endroits bien précis, y compris, au besoin, dans les bureaux individuels.

8/ Procédures garantissant les droits des personnes concernées ***(droits d'accès, de faire rectifier, de faire verrouiller, de faire effacer, d'opposition)***

Les personnes concernées peuvent faire valoir leurs droits d'accès à leurs données, de faire rectifier, de faire verrouiller, de faire effacer ces données et d'opposition en s'adressant par écrit au Chef de la Section sécurité et sûreté.

Sous réserve du droit d'opposition, ces droits peuvent faire l'objet d'une limitation conformément à l'article 20, paragraphe 1, du règlement n° 45/2001.

9/ Procédures de traitement automatisées/manuelles

Les caméras dissimulées respectent les caractéristiques suivantes :

- elles ne sont pas pourvues d'un système d'enregistrement sonore;
- elles sont indépendantes du système de vidéosurveillance générale géré depuis le poste de commandement de sécurité (PCS/PCI);
- elles peuvent être pourvues d'un système de détection automatique de mouvement.

Seuls les membres autorisés de la Section sécurité et sûreté peuvent poser et exploiter ces caméras dissimulées et ce, uniquement dans le cadre d'une investigation interne de sécurité et après décision du Greffier de la Cour de justice de l'Union européenne. Ceux-ci pourront y rechercher, le cas échéant, des éléments de preuve à charge ou à décharge.

10/ Support de stockage des données

a) Images filmées

Les images filmées sont stockées sur support informatique.
L'acquisition des images numériques se fait sur des cartes mémoire amovibles type SD (Secure Digital) ou équivalent. Seuls les membres autorisés de la Section sécurité et sûreté peuvent accéder à ces cartes et les exploiter.
Les images pertinentes sont conservées sur un PC isolé et dédié aux investigations internes de sécurité. Seuls les membres autorisés de la Section sécurité et sûreté peuvent exploiter ce PC avec accès par mot de passe et disque dur crypté.
Les images issues de caméras dissimulées ne transitent pas sur le réseau fédérateur de sûreté et ne peuvent pas non plus être transmises au PCS/PCI.

b) Registre électronique de conservation et des transferts

Les opérations de transfert des images et la conservation des images aux fins d'une investigation interne de sécurité sont documentées dans le registre électronique spécifique de conservation et des transferts. Ce registre est distinct de celui tenu pour la vidéosurveillance générale.

c) Registre papier des autorisations du recours à la vidéosurveillance dissimulée

La Section sécurité et sûreté tient un registre à jour avec toutes les autorisations de recours à la surveillance dissimulée.

11/ Base légale et licéité du traitement

Base légale:

Schéma directeur de mise en sûreté du complexe immobilier de la Cour de justice de l'Union européenne daté du 9 juin 2005, adopté sur décision du Comité Administratif le 1er juillet 2009.

Politique de vidéosurveillance de l'institution adoptée par le Directeur général des infrastructures de la Cour de justice de l'Union européenne le 26/05/2014 et en particulier le point *4.4. Surveillance dissimulée*.

Base de licéité:

Article 5, sous a), du règlement n° 45/2001.

12/ Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

- Fonctionnaires et agents de la Section sécurité et sûreté de la Direction des bâtiments (visualisation, enregistrement, copie, archivage, effacement) ;
- En outre, les données peuvent être communiquées à d'autres destinataires dans des cas particuliers :
  - la Cour de justice (Cour), le 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 ;

- 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 ;
- 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'une investigation interne 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 Contrôleur européen de la protection des données 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).

13/ Politique de conservation des données personnelles (ou catégories de données)

Les images sont visionnées endéans sept jours ouvrables suivant leur enregistrement afin d'en évaluer la pertinence.

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 fin de cette investigation et des procédures faisant éventuellement suite à celle-ci. Cette conservation est documentée dans un registre électronique, les justifications de la conservation des images y sont précisées.

Au cours de ladite investigation, la Section sécurité et sûreté procède une fois par mois à une réévaluation de la pertinence de toutes les images ainsi conservées compte tenu des autres éléments entre temps recueillis.

13 a/ Dates limites pour le verrouillage et l'effacement des différentes catégories de données (après requête légitime de la personne concernée)
(Merci d'indiquer les dates limites pour chaque catégorie, si nécessaire)

Verrouillage: 15 jours ouvrables, période pendant laquelle le responsable du traitement prend une décision sur la demande de verrouillage.

Effacement: 1 jour ouvrable après avis en ce sens du délégué à la protection des données ou du Contrôleur européen de la protection des données.

14/ Finalités historiques, statistiques ou scientifiques
Si vous conservez les données pour des périodes plus longues que celles mentionnées ci-dessus, merci d'indiquer, si nécessaire, ce pourquoi les données doivent être conservées sous une forme permettant l'identification.

Néant.

15/ Transferts de données envisagés

Tout transfert ou divulgation de données ne peut être effectué que par le responsable du traitement après consultation du délégué à la protection des données et, si ce dernier l'estime nécessaire, du Contrôleur européen de la protection des données.

Tout acte de transfert ou de divulgation de données à des destinataires extérieurs à la Section sécurité et sûreté est répertorié dans un registre électronique distinct de celui tenu pour le système de vidéosurveillance générale.

Dans les conditions définies par l'article 8 du règlement n° 45/2001, les images peuvent être transmises à la police luxembourgeoise si cela s'avère nécessaire aux fins d'une enquête menée par celle-ci dans l'exercice de ses compétences.

16/ Le traitement présente des risques particuliers qui justifient un contrôle préalable :

comme prévu à:

□ Article 27.2. (a)
Les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté,

□ Article 27.2. (b)
Les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement,

□ Article 27.2. (c)

Les traitements permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées pour des finalités différentes,

□ Article 27.2.(d)

Les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat,

X Autre (concept général de l'article 27.1)

17/ Commentaires

Néant.

Cour de justice de l'Union européenne, Luxembourg, le 26 mai 2014.

Délégué à la protection des données : Monsieur Agostino Valerio PLACCO

Signature du responsable du traitement : Mme Alexandra de MALEVILLE