EUROPEAN DATA PROTECTION SUPERVISOR

PETER HUSTINX
CONTRÔLEUR

Monsieur Mathieu THOMANN
Directeur de la sécurité et de l'évaluation des risques
Parlement européen
BRU - ASP 01H356
B-1047 Bruxelles

Bruxelles, le 17 décembre 2013
PH/UK/sn/D(2013)0632 **C 2013-0471**
Merci d'utiliser l'adresse edps@edps.europa.eu pour toute correspondance

Objet: **Notification en vue d'un contrôle préalable concernant la politique de vidéosurveillance adoptée par le Parlement européen (PE) le 20 avril 2013 (dossier 2013-0471)**

Monsieur,

Le 30 avril 2013, le contrôleur européen de la protection des données (le «CEPD») a reçu du délégué à la protection des données (le «DPD») du Parlement européen (le «PE») une notification en vue d'un contrôle préalable au titre de l'article 27 du règlement (CE) nº 45/2001 (le «règlement») sur les traitements liés au système de vidéosurveillance du PE tels qu'énoncés dans la politique de vidéosurveillance du PE (la «politique») adoptée le 20 avril 2013. Le CEPD avait été informé auparavant de l'adoption de la politique par une lettre du secrétaire général adjoint du PE en date du 26 avril 2013. Le CEPD a reçu un modèle de notification révisée et plusieurs annexes le 27 novembre 2013, ainsi qu'une version complète de la notification révisée comprenant toutes les annexes pertinentes le 13 décembre 2013.

Le CEPD se réjouit de l'adoption de la politique de vidéosurveillance du PE (la «politique»), qui marque un tournant dans la mise en œuvre des recommandations formulées dans les lignes directrices en matière de vidéosurveillance[1] (ci-après les «lignes directrices») publiées par le CEPD en mars 2010. En effet, ces lignes directrices invitaient les organes et institutions de

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

l'UE à mettre leurs pratiques existantes en conformité avec les lignes directrices avant le 1er janvier 2011.

À la lumière de la notification dans la version notifiée le 13 décembre 2013, le CEPD ne s'intéressera qu'aux pratiques du PE qui ne semblent pas être conformes aux principes du règlement et aux lignes directrices, et il limitera son analyse juridique à ces pratiques. Compte tenu du principe de responsabilité qui guide son action, le CEPD souhaiterait néanmoins souligner que *toutes* les recommandations pertinentes formulées dans les lignes directrices s'appliquent aux traitements mis en place dans le cadre du système de vidéosurveillance du PE.

Le chapitre 4.3 des lignes directrices expose les situations dans lesquelles le CEPD considère qu'une notification en vue d'un contrôle préalable au titre de l'article 27 du règlement est nécessaire pour aider l'institution à mettre en place des garanties supplémentaires de protection des données dans les cas où ses activités vont au-delà des opérations normales pour lesquelles les lignes directrices apportent déjà des garanties suffisantes.
Les situations visées au chapitre 4.3 des lignes directrices comprennent notamment le recours à la surveillance dissimulée. Comme souligné dans la notification adressée et au chapitre 4.4 de la politique, le PE envisage d'avoir recours, «*dans de rares cas et sans qu'il y ait de connexion avec le système de vidéosurveillance, ... pour une durée limitée, à un système autonome de surveillance dissimulée au cours d'enquêtes internes*» comme prévu au chapitre 6.11 des lignes directrices. Les traitements en cause sont donc soumis au contrôle préalable ex post en conformité avec l'article 27 du règlement.

Toutefois, comme l'a relevé le CEPD après la publication des lignes directrices[2], 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'examinera *pas* de manière exhaustive tous les aspects des pratiques de l'institution en matière de vidéosurveillance. Au lieu de cela, comme c'est le cas en l'espèce, le CEPD concentrera 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.

1. Procédure

La procédure a été notifiée en vue d'un contrôle préalable au titre de l'article 27 du règlement le 30 avril 2013. Des informations supplémentaires ont été demandées au DPD du PE le 2 mai 2013 et reçues le 23 mai 2013. Le dossier a été suspendu du 2 mai 2013 au 23 mai 2013, puis à nouveau du 16 juillet 2013 au 28 novembre 2013 (c'est-à-dire pendant 155 jours au total). Une réunion entre les services s'est tenue le 18 septembre 2013. Le délai de deux mois prévu à l'article 27, paragraphe 4, du règlement a été prolongé de deux mois supplémentaires le 3 décembre 2013 en raison de la complexité du dossier. Le CEPD a reçu un modèle de notification révisée et plusieurs annexes le 27 novembre 2013, ainsi qu'une version complète de la notification révisée comprenant toutes les annexes pertinentes le 13 décembre 2013. Conformément à l'article 27, paragraphe 4, du règlement, le présent avis doit être rendu dans un délai de deux mois, c'est-à-dire au plus tard le 3 février 2014.

[2] Voir les «Questions fréquemment posées en matière de vidéosurveillance: contrôle préalable», chapitre 5, consultable sur http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_FAQ_videosurveillance_EN.pdf.

2. Recours à la surveillance dissimulée

Faits

Selon le chapitre 4.4 de la politique, «*Aucune opération de surveillance ad hoc n'est prévue dans le cadre du système de vidéosurveillance. Toutefois, dans de rares cas et sans qu'il y ait de connexion avec le système de vidéosurveillance, le PE peut avoir recours, pour une durée limitée, à un système autonome de surveillance dissimulée au cours d'enquêtes internes. Le placement de ces caméras répond à des conditions strictes qui garantissent une incidence minimale sur la vie privée. Une notification en vue d'un contrôle préalable au CEPD..., indiquant les procédures spécifiques à suivre et les garanties supplémentaires de protection des données qui ont été mises en place, sera incluse dans l'annexe 9. En cas de doute quant à la protection des données pour des cas particuliers, le délégué à la protection des données sera consulté*».

Le projet de chapitre 4.4 de la politique (telle que notifiée le 13 décembre 2013) prévoit qu'«*aucune opération de surveillance ad hoc n'est prévue dans le cadre du système de vidéosurveillance. Toutefois, dans de rares cas d'intrusion régulière, de vol ou autres atteintes graves à la sécurité, le PE peut avoir recours, pour une durée limitée et sans qu'il y ait de connexion avec le système de vidéosurveillance, à un système autonome de surveillance dissimulée au cours d'enquêtes internes. Le placement de ces caméras répond à des conditions strictes qui garantissent une incidence minimale sur la vie privée: sous réserve d'une demande écrite officielle émanant de la personne responsable du secteur, d'une évaluation des risques et de l'impact du placement (afin de s'assurer que le niveau de risque compense l'impact sur le respect de la vie privée), ainsi que de l'autorisation écrite préalable du directeur de la sécurité et de l'évaluation des risques. La période maximale de placement de ces caméras est d'un mois, après quoi la procédure décrite ci-dessus doit être répétée.*
Une fois placées, ces caméras ne filmeront qu'à des heures prédéfinies et auront recours à la détection de mouvements. Les images ne seront visionnées que par les agents du PE chargés de l'enquête. Les images pertinentes seront conservées de façon sécurisée avec le dossier de l'enquête pendant une durée maximale de dix ans, tandis que toutes les autres images seront immédiatement supprimées.
À l'issue de l'enquête, les personnes qui ont été identifiées sur les images pertinentes pour l'enquête en sont informées. En cas d'infractions pénales ou de menaces pour des parties tierces, les données peuvent être transférées vers les services de sécurité d'autres institutions de l'UE ou aux autorités nationales compétentes. Un tel transfert est soumis à une évaluation rigoureuse de la nécessité ainsi qu'à l'autorisation préalable du directeur de la sécurité et de l'évaluation des risques. Un formulaire de protection des données est signé par la partie destinataire».

Le projet de chapitre 3 de la politique (telle que notifiée le 13 décembre 2013) précise en outre qu' «*en principe nous ne surveillons pas les espaces censés assurer un respect plus important de la vie privée tels que les bureaux individuels, les espaces de détente, sauf dans de très rares cas et sous réserve de conditions strictes telles qu'énoncées au chapitre 4.4. Les endroits où les attentes en matière de respect de la vie privée sont très élevées, tels que les sanitaires, ne sont jamais surveillés*».

Selon la notification (telle que notifiée le 13 décembre 2013), «*dans de rares cas d'intrusion irrégulière, de vol ou autres atteintes graves à la sécurité (signalées par la (les) personne(s) responsable(s) d'un secteur ou par des agents de la direction générale de la sécurité), le placement temporaire d'une caméra discrète et autonome peut être autorisé dans un endroit où normalement aucune caméra n'est présente, par exemple dans un bureau ou un cagibi, dans le cadre d'une enquête lancée officiellement.*

De telles caméras discrètes et autonomes ne seront placées qu'après une demande écrite officielle de la personne responsable du secteur, et suivant l'autorisation écrite préalable du directeur général de la sécurité. Ces caméras n'ont aucun lien entre elles et ne sont pas reliées au système de vidéosurveillance. Aucune caméra ne sera installée dans des endroits où les personnes s'attendent à un respect accru de leur vie privée, tels que les sanitaires».

Les procédures spécifiques à suivre sont énoncées dans des documents supplémentaires (les «documents de mise en œuvre»):

Un document intitulé «*Caméras discrètes pour la réalisation d'enquêtes au Parlement européen*», qui a été présenté en annexe 1 de la notification initiale, puis à nouveau dans le cadre de la notification révisée du 13 décembre 2013, stipule que le «*recours à ces caméras n'a lieu que s'il s'agit d'une mesure nécessaire pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales et/ou la sécurité publique de l'institution et des pays hôtes...*» et que le «*placement des caméras discrètes fait l'objet de la procédure suivante:*

(...)
Une fois la caméra placée et après son retrait, des règles supplémentaires s'appliquent: ...

(...)

Les informations supplémentaires fournies le 23 mai 2013, qui étaient constituées d'un texte principal, d'une analyse d'impact (annexe I) et d'un formulaire joint intitulé «*Analyse des risques et de l'impact du placement de caméras discrètes*», précisaient les aspects suivants:

(...)

Aspects juridiques

Comme indiqué au chapitre 6.11 des lignes directrices, «*du fait de son caractère secret, la surveillance dissimulée est hautement intrusive. Par ailleurs, elle n'a guère d'effet préventif et n'est souvent envisagée que comme un piège permettant de rassembler des preuves. Il convient donc d'éviter d'y avoir recours»*. Dans ce même chapitre des lignes directrices, les propositions d'exception à ce principe doivent être assorties d'une justification convaincante et d'une analyse d'impact, et elles doivent faire l'objet d'un contrôle préalable par le CEPD. Si nécessaire, celui-ci peut imposer des mesures spécifiques pour garantir la protection des données.

À cet égard, le CEPD se réjouit de l'analyse d'impact fournie le 23 mai 2013 en annexe I des informations supplémentaires, mais aussi du fait qu'une «analyse de risque et d'impact ad hoc» sera effectuée dans chaque cas par le renseignement d'un formulaire («*Analyse de risque et d'impact du placement de caméras discrètes*»).

a) Enquêtes sur une infraction pénale suffisamment grave
Les lignes directrices stipulent que la surveillance dissimulée doit être utilisée pour enquêter sur «*un délit suffisamment grave dans le cadre d'une enquête formelle, exigée ou autorisée par la loi...*».

Le CEPD souhaiterait rappeler qu'il est important d'établir, eu égard au principe de proportionnalité des traitements (article 4, paragraphe 1, point c), du règlement), quel type d'allégations et de preuves internes/externes peut justifier légalement une surveillance

dissimulée (en particulier quelles allégations et preuves peuvent étayer le soupçon raisonnable d'une infraction pénale suffisamment grave devant faire l'objet d'une enquête).

Le CEPD apprécie l'approche sélective adoptée dans la notification et dans le projet de chapitre 4.4 de la politique, qui limitent le recours à la surveillance dissimulée aux «*rares cas d'intrusion régulière, de vol ou autres infractions graves à la sécurité*».

b) Organe décisionnel

Conformément aux lignes directrices, le recours à la surveillance dissimulée doit être conforme à la loi et être autorisé formellement (i) par un juge ou un autre magistrat habilité à le faire en vertu des lois de l'État membre qui a demandé le recours à la surveillance dissimulée au sein de l'institution, ou (ii) par l'organe décisionnel supérieur compétent de l'institution conformément au règlement écrit et publiquement disponible de l'institution concernant le recours à la surveillance dissimulée (par ex. un comité exécutif supérieur).

Le CEPD note que la politique et les autres documents présentés avec la notification ne comportent aucune référence à une autorisation formelle d'un juge (ou un autre magistrat habilité à le faire en vertu des lois de l'État membre) *ayant demandé le recours à la surveillance dissimulée* au sein de l'institution. Dans le cas où le PE souhaiterait recourir à la surveillance dissimulée dans ces circonstances également, le CEPD suggère qu'il en soit fait mention dans la politique.

c) Période de conservation

Selon la notification, le PE distingue les images qui sont pertinentes pour une enquête de celles qui ne le sont pas.

L'analyse d'impact produite le 23 mai 2013 en annexe I des informations supplémentaires souligne que «*toute image dénuée de pertinence pour l'enquête doit être immédiatement supprimée. La pertinence des images doit être vérifiée (et celles-ci doivent être supprimées si elles ne sont pas pertinentes) au moins une fois par semaine*» (soulignement ajouté).

Selon la notification, le recours à la surveillance dissimulée est limité aux «*rares cas d'intrusion régulière, de vol ou autres infractions graves à la sécurité»* (voir le chapitre 2, point a), ci-dessus) et devrait être clairement limité aux enquêtes sur les infractions pénales suffisamment graves et manifestement circonscrites.

Conformément à cet objectif, le CEPD encourage le PE à vérifier les images d'une telle enquête dès que possible, puis à prendre une décision immédiate quant à la pertinence ou à la suppression des images (selon le cas).

4. Conclusions

Le CEPD recommande au PE d'adopter des mesures spécifiques et concrètes pour mettre en œuvre les suggestions, rappels et recommandations énoncés ci-dessus concernant la politique de vidéosurveillance du PE. Le CEPD invite le PE à joindre le présent avis à sa politique et à inclure une référence à celui-ci dans la politique.

En ce qui concerne les suggestions et les rappels mentionnés dans la présente note, le CEPD souhaiterait être informé de la situation concernant la conformité avec les lignes directrices et recevoir les informations demandées.

Afin de faciliter ce suivi, nous vous serions reconnaissants de bien vouloir transmettre au CEPD, dans un délai de trois mois à compter de la date de la présente lettre, tous les documents pertinents démontrant que toutes les recommandations et tous les rappels ont été mis en œuvre.

Cordialement,

(signé)

Peter HUSTINX

cc.: M. Secondo SABBIONI, DPD du Parlement européen