

## **Rapport contenant des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéo-surveillance (2003)**

Comme adopté par par le Comité européen de Coopération juridique (CDCJ) lors de sa 78<sup>e</sup> réunion (20-23 mai 2003)

### **INTRODUCTION**

Les comités du Conseil de l'Europe sur la protection des données souhaitent attirer l'attention sur certains aspects de la surveillance. Le Groupe de projet sur la protection des données (CJ-PD) du Conseil de l'Europe a donc demandé à un consultant, M. Giovanni BUTTARELLI (Secrétaire général de l'Office italien de la protection des données), de rédiger un rapport sur la protection des données en relation avec les activités de surveillance. Ce rapport reconnaissant que toute étude de la surveillance est liée à l'évolution technologique des moyens de contrôle et doit être replacée dans son contexte historique, il avait été décidé d'élaborer une liste de Principes directeurs portant spécifiquement sur la vidéo-surveillance, qu'il faudrait prendre en compte en relation avec la vidéo-surveillance.

Après avoir examiné le rapport et les principes directeurs de M. Buttarelli, le CJ-PD a accepté de réviser et de préciser certains de ces principes et a donc élaboré le texte suivant.

De nombreux organismes publics et privés ont de plus en plus recours, à des fins diverses et dans différents secteurs, à des systèmes de surveillance qui leur permettent notamment de contrôler la circulation des personnes et des biens et l'accès aux propriétés, mais aussi certaines manifestations, situations ou conversations, par le biais de réseaux téléphoniques ou électroniques, ou de systèmes installés sur place.

Les systèmes de surveillance conduisent souvent à recueillir des données à caractère personnel dont la collecte et/ou l'enregistrement n'est parfois pas le but recherché par le responsable du traitement des données de la surveillance.

Une très grande partie de ces activités fait appel à des dispositifs de vidéosurveillance qui posent des problèmes particuliers de protection des données.

Les informations collectées à l'occasion d'activités de vidéosurveillance incluent souvent des données (sous la forme d'images et de sons) qui permettent d'identifier, directement ou indirectement, les personnes concernées et de surveiller leur comportement. En outre, les techniques des systèmes de vidéosurveillance convergent de plus en plus avec d'autres technologies qui font naître de nouvelles préoccupations relatives à la protection de la vie privée et des données. Elles comprennent entre autres, les enregistrements sonores, les réseaux informatiques sans fils et à haute vitesse utilisés pour le transfert des images, les systèmes de reconnaissance automatique du visage intégrés à des bases de données informatisées qui peuvent identifier les personnes ou suivre leur trace, et les appareils qui permettent de « voir » derrière les vêtements et les murs, par exemple les dispositifs de reconnaissance thermique ou infra-rouge.

Les activités de vidéo-surveillance impliquant le traitement de données à caractère personnel entrent dans le champ d'application de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE N°108, ci-après dénommée Convention 108) – qui a été élaborée lorsqu'il est apparu clairement qu'il était nécessaire, afin de garantir une protection juridique efficace des données à caractère personnel, de développer de manière plus précise et plus systématique la référence générale au respect de la vie privée énoncée à l'Article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après CEDH).

Des droits et garanties complémentaires sont énoncés dans diverses recommandations du Conseil de l'Europe et, en particulier:

- a. la Recommandation N° R(87)15 sur l'utilisation des données à caractère personnel dans le secteur de la police ;
- b. la Recommandation N° R(89)2 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;
- c. la Recommandation N° R(95)4 sur la protection des données à caractère personnel dans le secteur des télécommunications ;
- d. diverses autres recommandations qui, si elles ne renvoient pas expressément à la vidéo-surveillance, contiennent des garanties et des règles qui sont pertinentes pour la protection des données à caractère personnel ainsi que pour la communication des données et les flux transfrontières de données.

La vidéo-surveillance n'est pas expressément couverte par ces instruments. Compte tenu du recours croissant à la vidéo-surveillance et de son évolution technologique, il convient de traiter ce sujet.

En conséquence, ces principes directeurs étendent et précisent les garanties qui s'appliquent aux personnes concernées, contenues dans les dispositions des instruments existants pour ce qui est du traitement des données à caractère personnel collectées au moyen de la vidéo-surveillance. Ils couvrent tout type d'activité de vidéo-surveillance permettant (au moyen d'un équipement technique) d'observer, de collecter et/ou de stocker de manière systématique des données à caractère personnel portant sur un ou plusieurs individus, plus particulièrement en ce qui concerne leur comportement, leur présence et/ou leurs déplacements. Ces principes directeurs devraient couvrir les activités de surveillance systématique, qu'elles soient permanentes ou occasionnelles (lors d'un événement spécifique), que les données à caractère personnel soient traitées en tout ou en partie de manière automatisée, et qu'elles fassent partie d'un système d'archivage ou qu'elles constituent un traitement non automatisé systématique.

Certains principes directeurs prévoient de nouvelles possibilités des technologies de l'information qui permettront un accès et une correction faciles sans révéler les données à caractère personnel des tierces personnes.

Il convient d'attirer l'attention sur le fait que, dans ces limites, ces principes directeurs contiennent des garanties en faveur des droits et libertés fondamentales pour tous, notamment le droit au respect de la vie privée tel qu'établi aux articles 5, 6 et 8 de la Convention 108 et à l'Article 8 de la CEDH et que des dérogations à ces droits en vertu de l'Article 9 de la Convention 108, qui ont été élaborées sur la base de l'Article 8 de la CEDH, sont possibles lorsqu'elles sont prévues par la loi et constituent une mesure nécessaire dans une société démocratique dans l'intérêt :

- a. de la protection de la sûreté de l'Etat, de la sécurité publique, des intérêts financiers de l'Etat ou de la répression des infractions pénales ;
- b. de la protection des personnes concernées ou des droits et libertés d'autrui.

Ces principes directeurs sont destinés à être diffusés le plus largement possible aux personnes susceptibles d'être soumises à la vidéo-surveillance et aux usagers de systèmes de vidéo-surveillance et autres techniques et dispositifs de surveillance. En outre, ils s'adressent aux Etats membres, aux fabricants, aux revendeurs, aux fournisseurs de services et d'accès et aux chercheurs afin que des logiciels et des technologies puissent être développés qui accordent une plus grande part aux droits fondamentaux des personnes concernées par la vidéo-surveillance. Il appartient aux États membres du Conseil de l'Europe de veiller à ce que ces principes soient respectés de manière aussi systématique que possible.

Ces principes directeurs pourraient également servir de base à d'autres activités de surveillance qui ne reposent pas sur l'utilisation d'appareils de vidéo-surveillance.

## **PRINCIPES DIRECTEURS**

Toute activité de vidéo-surveillance suppose de prendre les mesures nécessaires pour veiller à ce que cette activité soit conforme aux principes en matière de protection des données à caractère personnel, notamment :

- 1) de veiller à ce qu'elle soit menée de manière loyale et licite, à des fins légitimes, spécifiques et explicites. Les données à caractère personnel collectées au moyen de la vidéo-surveillance ne devraient pas être traitées par la suite de manière incompatible avec les buts pour lesquels elles ont été collectées ;
- 2) de n'utiliser de vidéo-surveillance que si, selon les circonstances, la finalité de cette dernière ne peut être atteinte par d'autres mesures portant moins atteinte au respect de la vie privée ; dans la mesure où celles-ci n'entraînent pas des coûts disproportionnés.
- 3) de recourir à la vidéo-surveillance de manière adéquate, pertinente et non excessive par rapport aux finalités déterminées et spécifiques recherchées dans les cas individuels, lorsque le besoin en a été démontré, afin d'éviter toute atteinte inconsidérée et injustifiée aux droits et libertés fondamentales des personnes concernées, par exemple à la liberté de circulation, et en veillant à respecter la vie privée, même dans les lieux publics<sup>(1)</sup> ;
- 4) de n'effectuer la vidéo-surveillance que de manière à ce que les personnes enregistrées ne soient pas reconnaissables si la finalité du traitement ne nécessite pas leur possible identification;
- 5) d'éviter que les données collectées ne soient indexées, comparées ou conservées sans nécessité. Dans les cas où il s'avère nécessaire de conserver les données, de veiller à ce qu'elles soient effacées dès qu'elles ne sont plus utiles à la finalité déterminée et spécifique recherchée ;
- 6) de ne pas se livrer à des activités de vidéo-surveillance si le traitement des données à caractère personnel risque d'aboutir à une discrimination contre certains individus ou groupes d'individus uniquement en raison de leurs opinions politiques, de leurs convictions religieuses, de leur santé ou de leur vie sexuelle, ou de leur origine raciale ou ethnique ;

7) de faire savoir clairement et de façon appropriée que des activités de vidéo-surveillance sont en cours, en indiquant leur finalité ainsi que l'identité des responsables<sup>(2)</sup>, ou en informant à l'avance les personnes concernées. Compte tenu des circonstances spécifiques, d'autres informations<sup>(3)</sup> devraient être fournies aux personnes concernées, lorsque cela est nécessaire pour garantir un traitement équitable des données à caractère personnel et ne va pas à l'encontre des finalités de la surveillance ;

8) de garantir que, pendant la période de stockage, l'exercice du droit d'accès aux données et, le cas échéant, du droit de rectification, blockage et/ou de suppression seront octroyés aux personnes concernées, à moins que cela ne suppose un travail disproportionné ;

9) de prendre toutes les mesures techniques et organisationnelles nécessaires pour préserver l'intégrité des informations collectées<sup>(4)</sup> ;

10) de prendre en compte, en cas de stockage par les autorités policières de données à caractère personnel recueillies par des méthodes automatiques de vidéo-surveillance, les principes de la Recommandation no. R (87) 15 concernant la réglementation de l'utilisation des données à caractère personnel dans le secteur de la police doivent en outre être pris en compte ;

11) de limiter le recours à des systèmes de vidéo-surveillance sur le lieu de travail à des exigences organisationnelles et/ou de production, ou à des fins de sécurité au travail. Ce système ne doit pas avoir pour but la surveillance délibérée et systématique de la qualité et de la quantité du travail individuel sur le lieu de travail.

Les employés ou leurs représentants devraient être informés ou consultés avant l'introduction ou la modification de tout système de vidéo-surveillance. Lorsque la procédure de consultation révèle qu'il y a un risque de violation du droit des employés au respect de leur vie privée et de la dignité humaine leur consentement<sup>(5)</sup> devrait être recherché. En cas de litige ou de revendication, les employés devraient pouvoir se servir des enregistrements réalisés ;

12) Si les données à caractère personnel sont enregistrées et conservées, elles devraient l'être, dans la mesure du possible, de manière à ce que la personne concernée puisse exercer son droit d'accès, en accord avec la législation sur la protection des données, sans avoir connaissance des informations concernant des tiers.

Notes :

(1) Les responsables de tels systèmes doivent donc déterminer si et dans quelle mesure les systèmes de vidéo-surveillance sont adaptés à leurs besoins en tenant compte de l'implantation géographique des caméras (quelles zones urbaines et quelles rues et pourquoi) et choisir les technologies à adopter en fonction de ces besoins (définition de l'image, capacité de zoom, miniaturisation des caméras) sans utiliser de dispositifs excessifs.

(2) Dans certains cas, le but poursuivi par la personne responsable du traitement des données et son identité ressortent clairement des circonstances. Cependant, dans quelques cas limités (par exemple la gestion de la circulation), il peut ne pas être possible de faire connaître à l'avance son identité.

(3) Les informations à fournir à la personne concernée peuvent aussi inclure les spécifications techniques du système choisi.

(4) Cela est particulièrement important en cas de numérisation puisque la modification des données ne peut pas être facilement décelée. Les informations collectées ne devraient être modifiées que pour des raisons valables et justifiées ; toute information modifiée devrait être signalée comme telle et l'information originale devrait être conservée.

(5) Par exemple, ce consentement pourrait être donné, conformément aux procédures prévues par la législation nationale en vigueur, par les syndicats ou les conseils syndicaux.