DELIBERATION N°2010-13 DU 3 MAI 2010 PORTANT RECOMMANDATION SUR LES DISPOSITIFS DE VIDEOSURVEILLANCE MIS EN ŒUVRE PAR LES PERSONNES PHYSIQUES OU MORALES DE DROIT PRIVE

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe ;

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la Recommandation du Conseil de l'Europe n° R (8 9) 2 du 19 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

Vu le Rapport du Comité Européen de Coopération Juridique du Conseil de l'Europe établissant les principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance, adopté le 20 – 23 mai 2003 ;

Vu la loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives ;

Vu l'ordonnance souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la loi n° 1.165 du 23 décembre 199 3, susvisée ;

Vu la loi n° 1.264 du 23 décembre 2002 relative aux activités privées de protection des personnes et des biens ;

Vu l'ordonnance Souveraine n° 15.699 du 26 février 2003 fixant les conditions d'application de la loi n° 1.264 du 23 décembre 200 2 relative aux activités privées de protection des personnes et des biens ;

Vu le Code civil ;

Vu le Code pénal ;

LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES,

Conformément à l'article 1er alinéa 1 de la loi n° 1.165 du 23 décembre 1993, les traitements automatisés ou non automatisés d'informations nominatives ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le titre III de la Constitution.

La Commission de Contrôle des Informations Nominatives, autorité administrative indépendante, a pour mission de veiller au respect de ces dispositions. A ce titre, elle est notamment habilitée à formuler toutes recommandations entrant dans le cadre des missions qui lui sont conférées par la loi.

Par la présente recommandation, la Commission estime opportun de préciser les grands principes de protection des informations nominatives applicables aux dispositifs de vidéosurveillance exploités par les personnes physiques ou morales de droit privé afin d'orienter les demandeurs d'autorisation dans leur démarche auprès d'elle.

I- Dispositions générales

De nombreux organismes privés ont de plus en plus recours à des systèmes de surveillance afin, par exemple, de contrôler la circulation des personnes, le transport ou la manutention de biens, l'accès aux propriétés, ou encore les accès ou le déroulement de manifestations ou de réunions. Ces systèmes utilisent des moyens, plus ou moins complexes, nécessitant le recours à des outils numériques et informatiques, voire à des systèmes de communications électroniques.

Les systèmes de surveillance conduisent souvent à recueillir des informations permettant d'identifier une personne physique déterminée ou déterminable, même si, parfois, l'objectif recherché ne vise pas à les identifier.

Parmi ces systèmes de surveillance, les dispositifs de vidéosurveillance soulèvent des problèmes particuliers en matière de protection des informations nominatives.

Les informations collectées à l'occasion d'activités de vidéosurveillance incluent souvent des données (sous la forme d'images) qui permettent d'identifier, directement ou indirectement, les personnes passant dans le champ d'une caméra, et, de surveiller leur comportement.

En outre, les systèmes de vidéosurveillance peuvent converger avec d'autres technologies qui font naître de nouvelles préoccupations relatives à la protection de la vie privée et des données nominatives. Elles comprennent, entre autres, les enregistrements sonores, le transfert plus aisé des données par le biais de réseaux informatiques sans fils et à haute vitesse, les systèmes de reconnaissance automatique de visages intégrés à des bases de données informatisées qui permettent de repérer, d'identifier des personnes, voire de les suivre sur un parcours, ou encore la vulgarisation des dispositifs de reconnaissance thermique ou infra-rouge, qui offrent la faculté de « *voir* » sous les vêtements et derrière les murs.

En l'absence de dispositions légales ou réglementaires encadrant ce genre de technologies, la Commission estime nécessaire de retenir les principes fondamentaux ci-après exposés, afin de veiller à la conformité des dispositifs de vidéosurveillance avec les dispositions de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives.

Les principes ainsi consacrés par la présente délibération s'appliquent aux dispositifs :

- mis en œuvre par des personnes physiques ou morales de droit privé, visées à l'article 6 de la loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives ;
- mis en œuvre par des organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public portés sur une liste établie par arrêté ministériel, telle que mentionnée à l'article 7 de la loi n° 1.165 susmentionnée ;
- mis en œuvre dans des établissements recevant du public, définis par l'article 4 de l'arrêté ministériel n° 67.264 du 17 octobre 196 7 relatif à la protection contre les risques d'incendie et de panique dans les établissements recevant du public ;
- mis en œuvre dans des établissements non ouverts au public ;
- permettant de traiter de manière automatisée, systématiquement ou occasionnellement, des informations ou données permettant d'identifier ou de rendre identifiables une ou plusieurs personnes physiques, plus particulièrement en ce qui concerne leur présence, leur comportement et/ou leurs déplacements.

Par ailleurs, la Commission tient à rappeler que, conformément aux principes directeurs adoptés par le Comité Européen de Coopération Juridique du Conseil de l'Europe :

« *Toute activité de vidéosurveillance 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 :*

- *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 vidéosurveillance ne devraient pas être traitées par la suite de manière incompatible avec les buts pour lesquels elles ont été collectées ;*

- *de n'utiliser de vidéosurveillance 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.*

- *de recourir à la vidéosurveillance 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 ;

- *de n'effectuer la vidéosurveillance que de manière à ce que les personnes enregistrées ne soient pas reconnaissables si la finalité du traitement ne nécessite pas leur possible identification ;*

- *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 ;*

- *de ne pas se livrer à des activités de vidéosurveillance 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 ;*

- *de faire savoir clairement et de façon appropriée que des activités de vidéosurveillance sont en cours, en indiquant leur finalité ainsi que l'identité des responsables, ou en informant à l'avance les personnes concernées. Compte tenu des circonstances spécifiques, d'autres informations 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 ;*

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

- *de prendre toutes les mesures techniques et organisationnelles nécessaires pour préserver l'intégrité des informations collectées ;*

- *de limiter le recours à des systèmes de vidéosurveillance 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 vidéosurveillance. 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 devrait être recherché. En cas de litige ou de revendication, les employés devraient pouvoir se servir des enregistrements réalisés ;*

- *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 ».*

II- La licéité du dispositif de vidéosurveillance

La loi n° 1.264 du 23 décembre 2002 relative aux activités privées de protection des personnes et des biens soumet, aux termes de son premier article, l'exercice des « *activités privées de surveillance (…) accomplies en vue d'assurer la sécurité des personnes »* à des conditions déterminées. « *Y sont également soumises les activités exercées au titre du service interne d'une entreprise* ».

Les articles 5 et 6 de cette loi prévoit, notamment, que « *l'exercice sur le territoire monégasque de toute activité visée à l'article 1er est subordonné à l'obtention d'une autorisation administrative préalable* », autorisation *« délivrée par le Ministre d'Etat. ».*

Aux termes de l'article 10-1 la loi n° 1.165 du 23 décembre 1993, susvisée, *« les informations nominatives doivent être collectées et traitées loyalement et licitement ».* La Commission considère, en conséquence, que cette autorisation administrative du Ministre d'Etat atteste du caractère licite de l'activité et des moyens utilisés.

Elle est donc, non seulement, un préalable obligatoire à toute saisine de la CCIN, mais aussi une pièce qui doit obligatoirement figurer dans le dossier déposé auprès d'elle au titre des formalités préalables à toute mise en œuvre de traitement automatisé d'informations nominatives, lorsque l'activité de protection implique un système de vidéosurveillance couplé d'un traitement automatisé d'informations nominatives.

III- La justification des dispositifs de vidéosurveillance

En application de l'article 10-2 de la loi n° 1.165 , la Commission considère que les traitements automatisés d'informations nominatives relatifs aux dispositifs de vidéosurveillance peuvent être justifiés lorsqu'ils sont mis en œuvre aux seules fins :

- de répondre à une obligation légale à laquelle est soumis le responsable de traitement ou son représentant ; ou,
- de permettre la réalisation d'un intérêt légitime poursuivi par le responsable de traitement ou son représentant ou par son destinataire, à la condition de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ; ou,
- de permettre la réalisation d'un but d'intérêt public poursuivi par les organismes privés concessionnaires d'un service public ou investis d'une mission d'intérêt général.

Elle estime également qu'un tel traitement peut être justifié par le consentement de la personne concernée. Néanmoins, elle appelle l'attention des responsables de traitement sur le fait que cette justification, qui sera apprécié de manière très stricte par la Commission, doit être étayée et expliquée, notamment, en cas de contrat de travail.

En outre, si le traitement est mis en œuvre à des fins de surveillance, le demandeur devra apporter les éléments permettant à la Commission de s'assurer que le traitement est « *nécessaire à la poursuite d'un objectif essentiel* » mis en exergue, et comment il s'est assuré que les droits et libertés des personnes seront protégés.

IV- Les fonctionnalités du traitement

La Commission considère que, compte tenu du caractère intrusif des dispositifs de vidéosurveillance traitant les informations nominatives et des informations qui peuvent y être associées, la mise en œuvre de tels dispositifs n'est admissible que dans le cadre des fonctionnalités suivantes :

- assurer la sécurité des personnes ;
- assurer la sécurité des biens ;
- permettre le contrôle d'accès ;
- permettre la constitution de preuve en cas d'infraction.

La Commission appelle l'attention des demandeurs sur le fait que ces systèmes ne peuvent donner lieu à d'autres utilisations (notamment commerciales). La communication de données personnelles enregistrées par une caméra est interdite sauf dans les cas prévus ou autorisés par la loi.

En outre, elle considère que le dispositif de vidéosurveillance ne doit pas :

- permettre de contrôler le travail ou le temps de travail d'un salarié ;
- conduire à un contrôle permanent et inopportun des personnes concernées.

Enfin, elle estime que l'installation de dispositif de vidéosurveillance est strictement interdite dans :

- les vestiaires, les cabinets d'aisance, les bains-douches, les cabines d'essayage ;
- les bureaux ainsi que dans tous lieux privatifs mis à la disposition des salariés à des fins de détente ou de pause déjeuner.

A ce titre, elle exige qu'un plan illustrant l'implantation des caméras avec mention des angles de vues soit impérativement joint au dossier déposé auprès de la CCIN.

V- L’information de la personne concernée

La Commission rappelle que l’existence d’un système de vidéosurveillance doit être portée à la connaissance des personnes concernées, conformément à l’article 13 de la loi n° 1.165, modifiée.

Ainsi, aux termes de l’article 14 de la loi n° 1.165 du 23 décembre 1993, modifiée, cette information doit comporter :

- l’identité du responsable de traitement et le cas échéant, celle de son représentant à Monaco ;
- la finalité du traitement ;
- l’identité des destinataires ou des catégories de destinataires des informations ;
- l’existence d’un droit d’accès aux informations les concernant.

La Commission estime donc que les personnes concernées doivent être informées de l’ensemble de ces mentions par tous moyens qu’il appartient au responsable de traitement de déterminer.

Nonobstant ces modalités d’informations, la Commission demande que l’information relative à l’exploitation d’un système de vidéosurveillance soit dispensée, dans tous les cas, par le biais d’un panneau d’affichage mentionnant l’existence de ce dispositif. Cet affichage doit garantir une information visible, lisible, claire et permanente de la personne concernée.

Ainsi, afin de satisfaire à cette exigence, ces panneaux, affichés à l’entrée des lieux filmés, doivent comporter, *a minima* :

- un pictogramme représentant une caméra ;
- le nom de la personne auprès de laquelle s’exerce le droit d’accès et les destinataires potentiels des informations.

VI- Les catégories d’informations traitées

Conformément aux principes relatifs à la qualité des informations nominatives, la Commission estime que seules les catégories d’informations suivantes peuvent être collectées et traitées :

- Informations relatives à l’identification de la personne concernée : image, visage, silhouette, voix ;
- Informations temporelles ou horodatage : lieux, identification des caméras, date et heure de la prise de vue ;
- Données d’identification électronique : Logs de connexion des personnels habilités à avoir accès aux images et au traitement.

VII- Les personnes ayant accès aux informations et les destinataires

La Commission estime que l'accès aux informations objet de ce traitement doit être limité aux seules personnes qui, dans le cadre de leurs fonctions, peuvent légitimement en avoir connaissance au regard de la finalité du dispositif.

Sur ce point, elle rappelle que, conformément aux dispositions du second alinéa de l'article 17-1 de la loi n° 1.165 précité e, le responsable de traitement doit « *déterminer nominativement la liste de personnes autorisées qui ont seules accès, pour les strictes besoins de l'accomplissement de leurs missions, aux locaux et aux installations utilisés pour les traitements, de même qu'aux informations traitées* ».

Cette liste doit impérativement être jointe au dossier de demande d'autorisation.

Les autorités judiciaires et policières peuvent être destinataires des informations objets du traitement dans le cadre des missions qui leur sont légalement et réglementairement conférées en cas de recherche de preuve ou de constatation d'infraction.

VIII- Les mesures de sécurité

La Commission considère que le responsable de traitement doit prendre toutes précautions utiles pour préserver la sécurité des informations objet du traitement dans le respect des dispositions des articles 17 et 17-1 de la loi n° 1.165.

Dans ce sens, elle rappelle que doivent être mises en place, « *des mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé* », et que ces mesures doivent « *assurer un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à protéger ».*

A ce titre, elle demande notamment que :

- soient mises en place des mesures de contrôle et d'identification des personnes habilitées à avoir accès aux informations conformément à l'article 30 de l'ordonnance souveraine n° 2.230 du 19 juin 2009 fi xant les modalités d'application de la loi n° 1.165 du 23 décembre 199 3, modifiée ;
- les personnes affectées à l'exploitation du système reçoivent des consignes strictes qui garantissent le respect de la confidentialité.

La Commission admet, qu'en raison de circonstances particulières tenant à la nécessité de prévenir ou de réprimer des atteintes aux personnes ou aux biens, des données puissent être extraites et/ou copiées afin d'être conservées sur un support distinct en vue de la communication des images et éléments d'identification aux autorités judiciaires ou policières légalement habilitées à en recevoir délégation.

A ce titre, la Commission demande que ce support et les informations qui y sont inscrites soient, jusqu'à sa destruction ou l'effacement des informations, protégés par des dispositifs et procédures de sécurité permettant d'une part, de chiffrer le support afin d'assurer la sécurité de l'accès aux informations aux seules personnes habilitées à y avoir accès et d'autre part, de garantir l'authenticité, la fiabilité et la lisibilité des données, en tenant compte de l'état de l'art.

IX- La durée de conservation

La Commission rappelle que les informations objet de la présente recommandation ne peuvent être conservées sous une forme permettant l'identification de la personne concernée que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées.

Ainsi, au regard des fonctionnalités énumérées au point 3 de la présente recommandation, la Commission estime qu'une durée de conservation d'un mois paraît proportionnée.

La durée de conservation des logs de connexion ne peut être supérieure à un mois sauf justification du responsable de traitement.

Elle estime par ailleurs que les informations communiquées sur le support aux fins de communication aux autorités judiciaires et policières peuvent être conservées jusqu'à la fin de la procédure judiciaire.

Après en avoir délibéré :

Rappelle que :

- les traitements automatisés d'informations nominatives liés à des dispositifs de vidéosurveillance mis en œuvre à des fins de surveillance ou portant sur des soupçons d'activités illicites, des infractions, des mesures de sûreté par les personnes physiques ou morales de droit privé sont soumis à l'autorisation de la Commission de Contrôle des Informations Nominatives ;
- seuls les traitements remplissant les conditions fixées par la présente recommandation pourront faire l'objet d'une autorisation de mise en œuvre.

Le Président,

Michel SOSSO