

Le dispositif légal de la vidéosurveillance dans les lieux publics

La vidéosurveillance est encadrée, en France, par la loi et une circulaire du ministère de l'intérieur. Les prescriptions techniques des systèmes de vidéosurveillance sont, quant à elles, définies par un arrêté.

La vidéosurveillance est encadrée, en France, par la loi n°95-73 du 21 janvier 1995 relative à la sécurité (modifiée par la loi du 23 janvier 2006), son décret d'application n°96-926 du 17 octobre 1996 (modifié par le décret du 28 juillet 2006) et une circulaire du ministère de l'intérieur du 22 octobre 1996. Les prescriptions techniques des systèmes de vidéosurveillance sont, quant à elles, définies par l'arrêté du 26 septembre 2006 portant définition des normes techniques et, plus récemment, par celui du 3 août 2007.

Régime applicable et finalité

Il convient de distinguer selon que la vidéosurveillance s'exerce sur la voie publique ou dans les lieux et établissements ouverts au public.

La transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéosurveillance relèvent du pouvoir des autorités publiques compétentes, c'est-à-dire celles qui ont la capacité d'exercer un pouvoir de police : préfet, maire, responsables d'établissements publics (SNCF, RATP, hôpitaux) ou de services publics (prisons), certains concessionnaires (sociétés d'autoroute)... (circulaire 96, Art. 2.3.1.1).

La finalité de la vidéosurveillance doit être limitée aux cas énumérés par le législateur : la protection des bâtiments et installations publiques et leurs abords, la sauvegarde des installations utiles à la défense nationale, la régulation du trafic routier et la constatation des infractions aux règles de la circulation, la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression et de vols et la prévention d'actes de terrorisme (L. 95, art. 10-II).

Elle doit également être respectueuse de la vie privée et, à ce titre, doit exclure la visualisation d'images de l'intérieur des immeubles d'habitation, et de façon spécifique, d'images de leurs entrées (L. 95, art. 10-II al.4).

Lorsque la vidéosurveillance s'exerce dans des lieux et établissements ouverts au public, elle devient « accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions » (comme l'acquittement d'un droit d'entrée) » (TGI Paris 23 oct. 1986, cité par Circ. 96, art. 2.3.2.1).

Cependant, sa finalité doit rester limitée à la sécurité des personnes et des biens. C'est le cas notamment des lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol (stations-service, banques, bijouteries, pharmacies, nombre d'agressions précédemment subies...) ou qui sont susceptibles d'être exposés à des actes de terrorisme.

Par ailleurs, en cas d'exposition à un risque terroriste, il est également possible pour les personnes morales autres que les « autorités publiques compétentes » de recourir à la vidéosurveillance pour assurer la protection des abords immédiats de leurs bâtiments et installations susceptibles d'être exposés à des actes de terrorisme (L. 95, art. 10-1, al. 3).

En cas d'urgence, l'autorisation peut être délivrée par le Préfet, sans avis préalable de la commission

départementale (L.95, art. 10-III bis). Cette dernière devra se prononcer dans les quatre mois qui suivent la délivrance de l'autorisation provisoire.

Normes techniques à respecter

La mise en oeuvre de la vidéosurveillance est subordonnée au respect des normes techniques précisées successivement par les arrêtés du 26 septembre 2006 et du 3 août 2007.

La première condition porte sur les caméras de vidéosurveillance qui doivent être « réglées, équipées et connectées au système de visualisation et, le cas échéant, au système de stockage, de façon que les images restituées lors de la visualisation en temps réel ou en temps différé permettent de répondre aux finalités pour lesquelles le système de vidéosurveillance a été autorisé ».

A ce titre, il convient de préciser les caractéristiques techniques pour atteindre les objectifs de sécurité, notamment le taux d'indisponibilité, le rôle des caméras (reconnaissance d'individus sur une zone donnée, identification pour ouverture...).

La deuxième condition concerne les conditions de transmission des images. La qualité des images restituées sera nécessairement dépendante de la qualité des caméras, des liaisons de données, de la capacité de compression des images...

La bande passante est un élément clé, toute insuffisance étant de nature à provoquer une perte préjudiciable d'informations ou une réduction du nombre d'images enregistrées par seconde. Si l'arrêté du 3 août 2007 ne donne aucune précision sur la notion de bande passante suffisante, il indique le poids moyen d'une image de qualité (45ko par exemple) et l'ordre de grandeur des capacités de bandes passantes.

Par ailleurs, la sécurité des réseaux exige la vérification des garanties d'intégrité (conformité aux images originelles), de disponibilité (accessibilité aux images et capacité de résistance aux agressions externes et aux dysfonctionnements possibles) et de confidentialité (accessibilité réservée aux seules personnes habilitées, mise en place de dispositifs - au moyen du chiffrement par exemple - contre l'interception et la lecture des données).

La troisième condition définit les contraintes liées au stockage des données. Le support de stockage doit ainsi être obligatoirement numérique dès lors qu'il y a huit caméras ou plus couvrant une entité géographique autonome. Il peut être indifféremment analogique ou numérique, lorsque le nombre de caméras est inférieur à huit. Cette contrainte ne vise que le module d'enregistrement des images. Ainsi la caméra ou encore le système d'enregistrement peut être analogique, à condition toutefois que le flux soit numérisé par la suite dans le premier cas et qu'il existe un système en double d'enregistrement numérique dans le deuxième cas.

Il faut encore que le système de vidéosurveillance permette de certifier la date, l'heure et l'emplacement de la caméra. A cet effet, deux méthodes sont possibles. La première consiste à prévoir un marquage direct sur l'image vidéo (avec l'inconvénient de masquer une partie de l'image). La seconde prévoit d'associer les informations au flux vidéo par une liaison logicielle. Dans les deux cas, il faudra démontrer la fiabilité du référentiel temporel associé aux images.

S'agissant du format et du nombre d'images enregistrées par seconde, le texte opère une distinction entre la notion de plan étroit (permettant d'analyser les informations sur des individus ou des objets présents dans le champ de la caméra) et celle de plan large (permettant de fournir une vue globale).

Il convient enfin de prévoir un journal de traçabilité des actions effectuées sur les flux. La fonction doit être numérique lorsque le système fonctionne avec huit caméras ou plus.

La quatrième condition traite des contraintes d'interopérabilité. Les opérations d'exportation sont déterminantes car elles peuvent être source d'une perte de qualité des images, par suite d'une modification du format ou du type de compression des flux vidéo.

A ce titre, l'arrêté du 3 août 2007 prévoit plusieurs mesures cumulatives : (i) la traçabilité des exportations qui permet l'identification des personnes qui ont exporté les flux vidéo se fait via un journal. Celui-ci peut être manuel en présence d'un système de vidéosurveillance analogique ou de moins de huit caméras. Il doit être électronique en présence de plus de huit caméras ; (ii) la disponibilité de supports de stockage pour remplacer ceux extraits du système ; ceci a vocation à permettre la poursuite de l'enregistrement en phase d'exportation ; (iii) l'utilisation de supports physiques d'exportation non réinscriptible et à accès direct, c'est à dire sans avoir à parcourir séquentiellement tout le support ; ces supports doivent être compatibles avec le volume des données (CD et DVD) ; (iv) la mise en place d'un logiciel d'exploitation des données, disjoint du support des données ; il doit permettre la lecture sans dégradation, en accéléré, au ralenti, en arrière, par arrêt sur image ainsi que la sauvegarde des images et séquences, dans un format standard et sans perte d'information. L'objectif est de pouvoir identifier la caméra, la date et l'heure d'enregistrement et de rechercher par caméra, date et heure.

Garanties de transparence et d'accès

La mise en oeuvre d'un système de surveillance exige également le respect de certaines garanties.

En premier lieu, le responsable du système doit préserver le droit d'accès, c'est à dire le droit de toute personne intéressée à obtenir accès aux enregistrements la concernant et le droit de vérifier destruction dans les délais prévus (L. 95, art. 10-V). Il n'est possible d'opposer un refus à une demande d'accès qu'en cas de risque d'atteinte à la sécurité de l'Etat, la défense, la sécurité publique...

Le public doit également être informé de manière claire et permanente de l'existence du système de vidéosurveillance et de l'autorité ou de la personne responsable (L. 95, art. 10-II al. 4). Sur la voie publique, cette information doit être apportée au moyen de panneaux comportant un pictogramme en forme de caméra.

Aucune règle ne précise les modalités d'affichage mais le décret de 1996 énonce des principes de clarté et de permanence (D. 96-926, art. 13-1) . Dans les lieux et établissements ouverts au public, des affiches ou panneaux doivent informer de l'existence d'un dispositif de vidéosurveillance. Par ailleurs, pour permettre l'exercice du droit d'accès, le responsable du système de vidéosurveillance doit être clairement identifié avec l'indication de son nom, sa qualité et son numéro de téléphone.

Enfin, il est prévu que les images enregistrées ne peuvent être conservées que pendant un délai maximum d'un mois^[1] (L. 95, art. 10-IV).

Contrôle et sanctions

Une commission départementale dispose d'un pouvoir de contrôle des conditions de fonctionnement des dispositifs autorisés (L. 95, art. 10-III al.6). Le non-respect des garanties apportées par la loi est sanctionné pénalement par des peines de prison (3 ans) et d'amende (45.000

€), ceci sans préjudice de l'application de l'article 226-1 du code pénal qui sanction également de peines de prison (1 ans) et d'amende (45.000 €) les atteintes volontaires à l'intimité de la vie privée d'autrui.

En marge de ce dispositif spécifique, il convient de rappeler que la loi informatique et libertés a également vocation à s'appliquer lorsque « *les enregistrements visuels de vidéosurveillance (...) sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, (...)* » (L. 1995, art. 10-I, égalt D. 1996, art. 5).

[\[1\]](#) *Ce délai expire le jour du dernier mois qui porte le même quantième que le jour de l'acte qui fait courir le délai. A défaut de quantième identique, le délai expire le dernier jour du mois (NCPC, art. 641). Tout délai expire le dernier jour à 24 heures (NCPC, art. 642).*