SOMMAIRE

À PROPOS DE LA VIDÉOSURVEILLANCE

La vidéosurveillance fait aujourd'hui partie intégrante de notre quotidien. Cependant, les multiples interventions sur le sujet, quelles soient politiques, associatives ou universitaires, ne permettent pas toujours une lecture claire du système de vidéosurveillance.

De quoi parle-t-on ?

La vidéosurveillance est composée d'un ensemble de caméras disposées dans l'espace public et/ou privé, dans le but de le surveiller. Les images ainsi obtenues par les caméras sont regardées en temps réel par des opérateurs et/ou stockées dans des systèmes informatiques.

Depuis l'adoption de la Loppsi 2[1], dans les textes, la vidéosurveillance est appelée « vidéoprotection ». En effet, selon le ministère de l'Intérieur, lors du vote de la loi, « *le mot de "vidéosurveillance" est inapproprié car le terme de "surveillance" peut laisser penser à nos concitoyens, à tort, que ces systèmes pourraient porter atteinte à certains aspects de la vie privée. Dès lors, il y a lieu de remplacer le mot "vidéosurveillance" par le mot "vidéoprotection", qui reflète plus fidèlement tant la volonté du législateur que l'action conduite en faveur de nos concitoyens.* »

Depuis quand le système de vidéosurveillance se développe-t-il ?

La vidéosurveillance s'est développée dans les années 1990 dans les commerces, les banques mais aussi les transports en commun. Les premiers systèmes destinés à surveiller l'espace public ont été installés en France, notamment en région parisienne, à Levallois-Perret (Hauts-de-Seine), en 1993. L'initiative du maire de cette commune, Patrick Balkany, pour mettre en œuvre la lutte contre la délinquance de rue, s'est effectuée en dehors de tout cadre juridique. Ce n'est qu'en 1995 que le législateur donnera une légalité aux systèmes de vidéosurveillance placés sur la voie publique.

Ainsi, ce sont les initiatives municipales destinées à lutter contre la délinquance, largement médiatisées, qui ont fait entrer la question de la vidéosurveillance dans le débat public. En retour, les politiques nationales de sécurité ont permis le développement de la vidéosurveillance au niveau municipal, notamment parce que des dispositions législatives encadrent l'installation de caméras de vidéosurveillance

[1] *Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.*

dans des lieux publics. En effet, la loi du 10 janvier 1995 soumet à autorisation l'installation de caméras de vidéosurveillance dans des lieux publics ainsi que dans des lieux privés ouverts au public. Cette loi a à la fois légitimé l'installation des dispositifs de vidéosurveillance de voie publique et encadré le recours à cette technique.

En 2006, la loi relative à la lutte contre le terrorisme a marqué une plus grande implication de l'État dans le développement de la vidéosurveillance, et en 2007 la loi relative à la prévention de la délinquance a prévu le triplement du nombre de caméras sur la voie publique ainsi qu'une participation de l'Etat dans le financement de celles-ci à hauteur de 50 % des frais d'installation. En 2011, la Loppsi 2 a encore favorisé son développement en augmentant la liste des motifs d'installation et des utilisateurs des images.

Aujourd'hui, les caméras sont donc omniprésentes dans notre quotidien : dans la rue, sur les routes, dans les parkings, dans l'enceinte des transports en commun RATP/SNCF, dans les aéroports, dans les banques, les entreprises, les centres commerciaux, dans nos halls d'immeubles, dans les stades, dans les collèges et lycées, etc.

Et nos voisins européens ?

Chez nos voisins européens, le constat n'est guère différent. A ce jour, Londres est la ville où la vidéosurveillance est la plus répandue. Est avancé le chiffre stupéfiant de 500 000 caméras installées dans la capitale anglaise, et de plus de 4 millions sur le territoire du Royaume-Uni. Néanmoins, un tel dispositif n'a pas su déjouer les attentats meurtriers de juillet 2005 qui ont fait 56 morts et 700 blessés à Londres. Et ce même dispositif peut être source d'erreurs dramatiques puisque quelques jours plus tard, la police londonienne a abattu un jeune brésilien qui avait été signalé à tort par la vidéosurveillance comme un poseur de bombes.

Sans postuler que les risques liés à la vidéosurveillance soient tous aussi graves, de nombreuses questions se posent quant aux atteintes à la vie privée et à la liberté de circuler.

Penser la vidéosurveillance à la lumière des dispositifs déjà en place, des résultats obtenus depuis leur activation et des lois en vigueur, tel est le sens du présent guide.

La LDH :

- qui admet que des systèmes de vidéosurveillance limités et réfléchis puissent constituer des outils au service de la sécurité quotidienne, de la lutte contre la délinquance et la criminalité, rappelle et maintient sa franche opposition à la multiplication anarchique de ces systèmes qui sont attentatoires à la liberté fondamentale de circuler sans entrave ni surveillance, à la vie privée, et sont un outil de contrôle social,

- considère que présenter la vidéosurveillance comme un outil de prévention (hormis dans certains lieux fermés comme les parkings) ou pouvant être utilisé en flagrance (arrestation du délinquant pris sur le fait) constitue une politique dangereuse dans la mesure où elle induit des attentes des citoyens qui ne peuvent qu'être déçus ;

- constate et dénonce la carence de l'Etat concernant la communication d'informations sur ce sujet. Ce grave déficit d'information est à comparer à la volonté continue de multiplier ces instruments de vidéosurveillance, en remplacement de personnel de police ;

- déplore une telle position qui porte atteinte à la transparence que devrait manifester le ministère de l'Intérieur dans ce domaine, si ces choix étaient aussi légitimes et pertinents qu'il le prétend ;

- dénonce le fait que le législateur n'ait eu de cesse d'augmenter le périmètre soumis à surveillance, sans accorder dans le même temps aux citoyens des droits équivalents à l'augmentation du contrôle ;

- considère que les comités d'éthique ne sont qu'un leurre destiné à donner une illusion de fonctionnement démocratique à l'installation des systèmes de vidéosurveillance et réaffirme son opposition à toute participation.

La LDH demande que :

- la totalité des systèmes de vidéosurveillance soit, dans les plus brefs délais, placée sous le contrôle exclusif de la Cnil ;

- un fichier national des traitements et des caméras – chaque caméra étant individuellement identifiée avec indication de sa localisation – soit mis en place pour recueillir des informations sur toute nouvelle installation ;

- ce fichier des localisations soit public, et notamment accessible par Internet, afin que chaque citoyen puisse aisément s'assurer que la caméra qui le filme a été régulièrement installée et fait l'objet d'un contrôle légal ;

- soit interdit l'usage de drones et de logiciels permettant la reconnaissance faciale et l'analyse du comportement. Ces interdictions devront être pénalement sanctionnées de manière à ne pas permettre l'installation d'outils non seulement de surveillance mais de répression sur l'ensemble du territoire ;

- un audit parlementaire de la politique de multiplication des systèmes de vidéosurveillance permette d'évaluer le rapport coût/efficacité ainsi que les profits pour les lobbies militaro-industriels.

1

ÉTAT des LIEUX

Actuellement, trois systèmes de vidéosurveillance sont en service dans l'espace public et dans l'espace privé ouvert au public :
- les caméras reliées par câble, fibre optique ou wifi, à des postes d'observation – en général des centres de supervision urbain (CSU) – qui rassemblent plusieurs écrans sur lesquels s'affichent les images de plusieurs caméras. Les écrans sont surveillés par des opérateurs, sans enregistrement des informations ;
- les caméras, sur la base d'un système identique au précédent, mais avec enregistrement et stockage des informations ;
- les caméras non reliées à des écrans mais qui enregistrent et stockent les informations.

À cela s'ajoute le fait que les systèmes peuvent être équipés de logiciels permettant la détection des mouvements, le comptage des individus, l'association d'alarmes ou avertissements sonores à destination des « contrevenants », l'identification des plaques d'immatriculation, etc. En outre, les systèmes à venir tendent vers la mise en place de logiciels de détection automatique de comportements qualifiés d'« anormaux ».

L'amélioration constante des techniques, (caméras numériques et télécommandées, rotation à 360° sur sollicitation de l'opérateur, zoom jusqu'à 500 m), de la qualité des images fournies par les caméras et des logiciels permet d'envisager aujourd'hui des systèmes de surveillance de plus en plus pointus et dangereux pour les libertés. Et ce, pour plusieurs raisons :
- **la sélection automatique de caractéristiques de tri** dans les images enregistrées, sur la base de la couleur des vêtements, des cheveux, du port de lunettes, d'une barbe, etc. ;
- **la reconstitution automatique des déplacements d'une personne** donnée à partir de plusieurs caméras avec des champs de prise de vues non contigües ;
- **la détection des comportements**. Il s'agit de l'analyse de démarches ou de trajectoires « suspectes », de posture, direction, vitesse, localisation par rapport à un objet ou une personne ;
- **l'identification d'une personne**, sachant que selon l'institut de recherche criminelle de la gendarmerie nationale, l'identification faciale n'est possible qu'à partir d'un minimum de 25 pixels entre les deux yeux. Les caméras actuelles ne permettent pas de les obtenir ;
- **l'identification par l'image de l'iris**. Les caméras actuelles permettraient de fournir une image correcte jusqu'à trois mètres pour un sujet immobile. Cependant, cela est totalement insuffisant pour un sujet en mouvement.

Les travaux de recherche s'orientent vers une amélioration de la précision des caméras et la performance des logiciels d'analyse et de traitement des images. Déjà, au Royaume-Uni, des caméras sont capables de s'adresser à une personne dont la voix forte aurait été repérée ou la démarche suspecte aurait été détectée, et de lui

délivrer un message préenregistré de mise en garde ou de déclencher l'envoi d'une patrouille de police.
Dans ce contexte, la vidéosurveillance – présentée comme un outil de prévention – devient un outil de profilage et de répression puisque le logiciel lui-même est capable d'analyser un comportement « anormal » et d'en tirer un enseignement en vue de faire corriger ce comportement.
A ce stade, la question essentielle est : **comment et sur quelle base détermine-t-on un comportement « anormal » ?**

A. LES DOMAINES D'UTILISATION

1. SUR LA VOIE PUBLIQUE

La loi Loppsi 2 prévoit que la transmission et l'enregistrement des images prises sur la voie publique, par le moyen de la vidéosurveillance, peuvent être mis en œuvre par les autorités publiques compétentes aux fins d'assurer :
a. la protection des bâtiments et installations publics et de leurs abords ;
b. la sauvegarde des installations utiles à la défense nationale ;
c. la régulation des flux de transport ;
d. la constatation des infractions aux règles de la circulation ;
e. la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions ;
f. la prévention d'actes de terrorisme ;
g. le secours aux personnes et la défense contre l'incendie ;
h. la sécurité des installations accueillant du public dans les parcs d'attraction.

Il est assez significatif de constater que, dans les objectifs de la « vidéoprotection », la prévention des atteintes aux personnes n'est mentionnée qu'en cinquième position dans le texte de loi, bien après la sauvegarde du patrimoine et les infractions aux règles de circulation.

Toutefois, les caméras de vidéosurveillance sur la voie publique ne doivent pas visualiser l'intérieur des immeubles d'habitation ni même leurs entrées. Des procédés de masquage irréversible de ces zones doivent donc être mis en œuvre.

2. DANS LES COMMERCES

Des systèmes de vidéosurveillance peuvent être installés par des commerçants pour lutter contre les vols de marchandises par les clients ou les employés. En fonction des zones, les règles sont différentes. Il est bien entendu interdit d'installer des caméras à l'intérieur des cabines d'essayage ou dans les toilettes.

Les images enregistrées ne doivent être accessibles qu'à la direction du magasin, aux responsables et aux agents de sécurité. Il peut néanmoins y avoir autorisation de filmer la zone marchande avec une possibilité de visualisation des images en direct par tous les salariés et les clients. En revanche, la vidéosurveillance ne doit pas être utilisée pour surveiller le travail des salariés.

Les images peuvent être enregistrées et conservées un mois maximum.

Les systèmes de vidéosurveillance filmant les parties ouvertes au public (entrée et sortie, zones marchandes, caisses, etc.) doivent faire l'objet d'une autorisation du préfet. Quant aux systèmes filmant les zones non ouvertes au public (réserves, zones réservées au personnel, etc.), ils doivent faire l'objet d'une déclaration à la Cnil, s'ils permettent l'enregistrement d'images.

3. AU TRAVAIL

Des caméras peuvent être installées sur un lieu de travail pour contribuer à la sécurité des biens et des personnes, à titre dissuasif ou pour identifier les auteurs de vols, de dégradations ou d'agressions. Elles ne peuvent en aucun cas entrainer une surveillance constante et permanente des salariés.

Les caméras peuvent être installées au niveau des entrées et sorties des bâtiments et des voies de circulation. Elles ne doivent pas filmer les employés sur leur poste de travail, ni filmer les zones de pause ou de repos des employés, ni les toilettes. De même, elles ne doivent pas filmer les locaux syndicaux ou des représentants du personnel.

4. DANS LES ÉTABLISSEMENTS SCOLAIRES

Des caméras peuvent être installées à l'intérieur d'un établissement à des fins de sécurité des biens et des personnes (lutte contre les violences, les dégradations, les vols, etc.) ainsi qu'à l'extérieur pour renforcer la sécurité de ses abords. Les caméras peuvent également filmer les accès de l'établissement (entrées et sorties) et les espaces de circulation.

Par respect pour la vie privée des élèves et des enseignants, il est exclu de filmer les cours de récréation, les salles de classe, la cantine, etc. pendant les heures d'ouverture. Les systèmes de vidéosurveillance doivent rester d'usage limité.

Pour les écoles, la décision d'installation est prise par les communes. Pour les collèges et lycées, la décision est du ressort du chef d'établissement après délibération du conseil d'administration compétent sur les questions relatives à la sécurité.

Les images enregistrées sont accessibles aux seules personnes habilitées, en principe le chef d'établissement, qui devraient être formées aux règles encadrant les systèmes de vidéosurveillance.

Les formalités à accomplir peuvent varier en fonction des lieux qui sont filmés. Si les caméras filment l'intérieur de l'établissement scolaire et permettent l'enregistrement

des images, le dispositif doit être déclaré à la Cnil. Si les caméras filment les abords de l'établissement et en partie la voie publique, le dispositif doit être autorisé par le préfet du département.

5. DANS LES IMMEUBLES D'HABITATION COLLECTIVE

Des dispositifs de vidéosurveillance peuvent être installés pour lutter contre les vols ou les dégradations dans les parties communes des immeubles d'habitation collective. Ces dispositifs peuvent filmer les espaces communs, à savoir le hall d'entrée, les portes d'ascenseur, la cour, le parking souterrain. En revanche, ils ne doivent pas filmer les portes des appartements ni les balcons ou terrasses des habitants.

Seuls le syndic, les membres du conseil syndical, le gestionnaire de l'immeuble ou le gardien doivent pouvoir visualiser les images. Les images ne devraient être consultées qu'en cas d'incident (vandalisme, dégradation, agression, etc.). Elles ne doivent en aucun cas servir à « surveiller » en temps réel les allées et venues des résidents ou des visiteurs.

Les propriétaires d'immeuble peuvent transmettre, de manière occasionnelle et en temps réel, les images enregistrées – à l'exception des entrées et des habitations – à la police ou à la gendarmerie s'ils redoutent des atteintes aux biens ou aux personnes. Une convention doit alors être conclue entre le préfet, le gestionnaire de l'immeuble (logement social) ou le syndic et le maire. L'existence de ce système de vidéosurveillance et la possibilité de transmission des images aux forces de l'ordre devront être affichés sur place. La durée de conservation des images est d'un mois maximum.

Les formalités à accomplir peuvent varier en fonction des lieux qui sont filmés :
- si les caméras filment des lieux uniquement accessibles aux personnes autorisées (par exemple, l'accès au hall d'entrée s'effectue avec une clé détenue uniquement par les occupants de l'immeuble) et permettent l'enregistrement des images, le dispositif doit être déclaré à la Cnil. En effet, les lieux sont alors considérés comme non ouverts au public. Cette déclaration doit être effectuée au nom du syndicat des copropriétaires ou du gestionnaire de l'immeuble ;
- si les caméras filment un lieu accessible à toute personne (en raison de l'absence de digicode, par exemple), une demande d'autorisation doit être faite à la préfecture. Ces installations doivent être votées à la majorité des copropriétaires. Un panneau affiché de façon visible doit informer les habitants.

6. À DOMICILE

Les particuliers peuvent installer des caméras de vidéosurveillance dans leur domicile pour en assurer la sécurité intérieure. Ces dispositifs ne sont pas soumis à la loi « Informatique et libertés » ni au Code de la sécurité intérieure. Cependant, pour respecter la vie privée des voisins et des passants, les systèmes ne peuvent filmer que l'intérieur de la propriété. Il est interdit de filmer la voie publique. Dans le cas où des salariés travaillent au domicile vidéosurveillé à plein temps ou ponctuellement (garde d'enfants, personnel médical, aides ménagères, etc.), les règles du Code du travail doivent s'appliquer, à savoir la déclaration à la Cnil et l'information du salarié.

B. COMBIEN DE CAMERAS

La Cnil, dans un article du 21 juin 2012[2], estime à 935 000 le nombre de caméras installées en France dans la rue, dans les magasins, les transports en commun, les bureaux, les immeubles d'habitation. Et la commission précise qu'il est « *difficile d'y échapper* ».

Dans ce même article, la Cnil indique : « *On compte 897 750 caméras autorisées depuis 1995, dont 70 000 pour la voie publique et 827 749 pour les lieux ouverts au public (chiffres issus du rapport 2011 du ministère de l'Intérieur relatif à l'activité des commissions départementales). La Cnil a reçu, quant à elle, 35 000 déclarations de dispositifs depuis 1978 (pouvant être constitués de une à plusieurs dizaines de caméras). Ceux-ci concernent principalement la vidéosurveillance au travail.* »

1. À PARIS

Selon la Cour des comptes[3], « *le réseau de vidéosurveillance de la voie publique ne comprenait [en 2010] que 293 caméras (non compris les caméras couvrant les réseaux de transports en commun ou celles installées au Parc des princes, aux abords du stade de France, au Forum des Halles et au Carrousel du Louvre), technologiquement dépassées et inadaptées à la lutte contre la délinquance. Un projet visant à installer 1 007 caméras à compter de 2011 a été engagé sous maîtrise d'ouvrage de l'Etat et non de la ville.* »

De son côté, Jean-Marc Manach[4] indique que les travaux – à savoir la mise en place de fibre optique, érection de pylônes pour fixer les appareils – devraient durer jusqu'à la fin de l'année 2012. Les commissariats de chaque arrondissement seront équipés pour accéder aux images. En effet, jusqu'à présent, les images ne sont visibles qu'à la préfecture de police. Ce système de vidéosurveillance ne comprendra pas moins de 400 kilomètres de fibre optique pour relier 55 sites dans Paris et la DCRI à Levallois.

Selon la préfecture de police, « *pour surveiller ces 1 000 caméras de vidéosurveillance, ainsi que les 13 000 caméras hors voie publiques (les 9 500 caméras du réseau de transport de la RATP ainsi que celles de sociétés privées, les grands magasins, par exemple qui ont signé une convention avec l'Etat), ce ne sont pas moins de 2 500*

[2] *Cnil, Actualités, article du 21 juin 2012, « Vidéosurveillance/vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée » - Site : www.cnil.fr*
[3] *Cour des comptes, rapport 2011, sur « l'organisation et la gestion des forces de sécurité publique » - in pages 140 et suivantes - Site : www.ccomptes.fr*
[4] *Article - janvier 2011 « A Paris, la police aura des yeux partout » - Site : http://owni.fr*

policiers et pompiers qui seront formés. » Le préfet Didier Martin, alors en poste en qualité de secrétaire général pour l'administration de la préfecture de police de Paris, a précisé en 2011 que ces policiers et pompiers « *seront les seuls à pouvoir accéder aux images et ils devront s'identifier avec une carte à puce. Leurs interventions seront donc tracées.* »

2. EN ILE-DE-FRANCE

La Cour des comptes recensait « *895 caméras dans les départements de la grande couronne parisienne avec 19% des communes (63 sur 334) équipées.* » La cour des comptes a comparé ce chiffre à ceux des Etats-Unis : « *… si la vidéosurveillance des espaces privés est très répandue, le nombre de caméras de voie publique dans les trois plus grandes villes américaines (500 à New-York, 200 à Chicago, 80 à Los Angeles) est modeste au regard de la population couverte (15 millions d'habitants).* »

3. ÉVOLUTION

Depuis 2008, les instructions ministérielles aux préfets portant sur les objectifs annuels de la politique de sécurité intérieure leur ont systématiquement rappelé l'objectif de tripler le nombre de caméras installées sur la voie publique. Ces instructions leur ont également demandé de mettre en œuvre un « plan départemental de développement de la vidéoprotection » dans les sites les plus sensibles. L'objectif n'est donc pas tant de tripler le nombre de caméras sur la voie publique, mais d'en interconnecter des dizaines, voire centaines de milliers (les caméras dans les magasins, les banques, les administrations, etc.).

Le 10 mars 2011, le Conseil constitutionnel a censuré la disposition de la Loppsi 2 qui prévoyait que toutes les personnes morales de droit privé (un syndicat de copropriétaires, une entreprise, un commerce …) auraient pu placer des caméras dans la rue, au-delà de leurs murs, aux abords de leur bâtiment, donc sur la voie publique, avec transmission possible des images, en temps réel, à la police. Une telle disposition aurait permis de déléguer à des personnes ou des sociétés privées la surveillance générale de la voie publique qui doit rester une compétence de la « force publique ».

Néanmoins, s'agissant de l'espace public, le préfet pourra imposer aux maires une vidéosurveillance temporaire en cas de risque particulier d'atteinte à la sécurité et de terrorisme. Compte-tenu de l'investissement technique financier qu'engendre l'installation d'un système de vidéosurveillance, il est possible de douter du caractère « temporaire » de celle-ci, si elle est réalisée.

Toutefois, le nouveau ministre délégué chargé de la Politique de la ville, François Lamy, a annoncé que le soutien de l'Etat au développement de la vidéosurveillance ne sera plus érigé au rang de priorité dans le Fonds interministériel de prévention de la délinquance (FIPD). Pour mémoire, en 2011, le FIPD a consacré 30 millions de son budget total à la vidéosurveillance. Ainsi en 2013, l'enveloppe « vidéosurveillance » sera divisée par trois au profit des actions sociales[5] .

[5] *La Gazette des communes, octobre 2012 - Site : www.lagazettedescommunes.com/132857/banlieues-entretien-exclusif-avec-francois-lamy-ministre-delegue-charge-de-la-politique-de-la-ville/*

2

QUELS RÉSULTATS ?

A. À L'ÉTRANGER

Aux Etats-Unis, en 2002, certaines grandes villes constataient que la vidéosurveillance s'avérait moins efficace pour combattre la petite et la grande délinquance par rapport à ce que les autorités fédérales pensaient initialement. C'est ainsi que des villes telles qu'Atlantic City, Miami ou Mount Vernon ont purement et simplement abandonné l'usage systématique de caméras de vidéosurveillance.

En Grande-Bretagne, le constat est sensiblement identique, même si le maintien du dispositif demeure encore important dans ce pays. Le cas de la Grande-Bretagne est particulièrement intéressant car les systèmes ont été implantés plus tôt et plus massivement qu'en France, notamment pour lutter contre les attentats de l'Ira. En outre, les implantations sont beaucoup mieux acceptées par la population qui n'hésite pas à mettre en œuvre le « neighborhood watch », qui est l'équivalent à grande échelle de nos « voisins vigilants ». Ainsi, le nombre de caméras urbaines est de trois à cinq fois supérieur à celui de la France.

Que l'objectif des systèmes soit la prévention (baisse du volume de la délinquance) ou la répression (augmentation du taux d'élucidation), la vidéosurveillance n'est efficace que si certaines conditions sont réunies : des ressources suffisantes et performantes, la mesure de la complexité de l'espace urbain, la combinaison de diverses mesures de prévention, la définition de cibles et d'objectifs pertinents, etc.

Un rapport de septembre 2006 de l' « Information Commissionner's Office », l'équivalent de la Cnil en Grande-Bretagne, qui fait lui-même suite à un rapport du ministère de l'Intérieur britannique, est éloquent. Outre rappeler le budget consacré à la mise en place de ces caméras au cours des dix dernières années, il soulige que l'étude du ministère de l'Intérieur a prouvé que les systèmes de vidéosurveillance qui ont été évalués avaient en général peu d'impact sur les niveaux de criminalité.

B. EN FRANCE

La commune de Levallois-Perret est significative des limites de ce dispositif. En 1993, 96 caméras sont installées dans la ville. Trois millions d'euros ont été investis pour cette mise en place, et 30 000 euros supplémentaires sont à ajouter pour l'entretien annuel du matériel. Deux ans plus tard, le maire de la commune demande un audit sur la sécurité aux fins d'évaluation du dispositif. Cette enquête conclut à « *un coût de fonctionnement considérable au regard de la fonctionnalité de l'outil mis en place, ainsi que sont inutilité totale au vu du projet initial.* »

Il en va de même pour la ville d'Amiens. Cette ville dispose d'un système de vidéo-surveillance de voie publique doté de 48 caméras, dont 85% sont situées au centre ville. En 2008, il était prévu de porter ce nombre de 48 à 100 caméras. Cependant, la nouvelle municipalité élue a d'abord souhaité lancer une évaluation afin de mesurer l'efficacité du dispositif.
L'étude, présentée au conseil municipal du 20 septembre 2012, souligne que « *malgré la présence d'un dispositif dense, la vidéoprotection ne semble pas avoir d'impact dissuasif ».* Et de conclure que *« l'utilité en matière de prévention de la délinquance pour une grande partie des caméras du centre ville s'avère donc secondaire* ».

Alors que de nombreuses grandes agglomérations ont installé des systèmes de vidéo-surveillance depuis plusieurs années, aucune étude officielle fiable n'a été réalisée en France. La réponse aux questions sur le sujet demeure invariable : « Cela fait baisser la délinquance », sans qu'aucune statistique ne vienne confirmer le propos.

1. RAPPORT SUR L'EFFICACITÉ DE LA VIDÉOPROTECTION

En juillet 2009, le ministère de l'Intérieur a publié un rapport intitulé « Rapport sur l'efficacité de la vidéoprotection », rédigé conjointement par l'Inspection générale de la police nationale, l'Inspection générale de l'administration et l'Inspection de la gendarmerie nationale. Il s'agit d'une étude administrative destinée à justifier des décisions antérieures. Elle ne remplit pas les conditions scientifiques d'évaluation, et ne saurait donc être recevable.

Pourtant ce rapport étayera la publication, en novembre 2010, d'un guide méthodologique de la vidéoprotection[6] destiné « *(…) à tout responsable ayant à piloter pour la première fois un projet de vidéoprotection, ayant l'intention de le faire ou souhaitant développer ou améliorer un dispositif existant (…)* ».

[6] *Site : http:/www.interieur.gouv.fr/sections/avotreservice/video-protection/guide-methodologique*

Les rapporteurs ont systématiquement présenté les chiffres sous forme de pourcentage, sans les valeurs absolues. L'impact de la vidéosurveillance a été mesuré en s'appuyant sur les chiffres de la délinquance générale enregistrée. Ces chiffres recouvrent pourtant des délits très divers. Il est donc difficile d'en tirer un quelconque enseignement, sachant que l'impact de la vidéosurveillance est nul sur des infractions telles que les chèques volés, les infractions économiques ou au Code du travail, les violences domestiques, etc.

A la question de l'efficacité de la vidéosurveillance sur la prévention de la délinquance, le rapport répond positivement. Il s'appuie sur une analyse comparative entre les chiffres globaux de la délinquance de l'ensemble des villes équipées avec toutes celles qui ne le sont pas. Or, les conditions d'une véritable évaluation scientifique doivent prendre en compte trois critères :
- l'étude de cas doit être contextualisée, afin d'isoler l'effet propre à la vidéosurveillance au regard d'autres variables telles que l'amélioration de l'éclairage public, le renforcement des effectifs policiers ou encore un changement de leurs modes d'action ;
- la comparaison entre plusieurs espaces semblables pour tenir compte des différents types de lieux où sont implantées les caméras : parkings, rues, quartiers d'habitat social, lycées, etc. ;
- l'analyse des statistiques des crimes et délits doit se faire par types d'infractions (étudier les chiffres des différents types d'infractions et éviter la présentation en pourcentages globaux qui ne permet pas de rendre compte de la réalité), et ce sur une période de deux ans minimum, avant et après l'installation des caméras.

A la question du déplacement de la délinquance des zones vidéosurveillées vers des zones non couvertes (effet « plumeau »), le rapport affirme que la vidéosurveillance a un « *effet plumeau… globalement faible* », et que « *l'impact en prévention dépasse le périmètre des zones vidéoprotégées*. » Or, le rapport du ministère de l'Intérieur se contente de comparer l'évolution de la délinquance dans une même circonscription de police ou de brigade de gendarmerie. Les témoignages de gendarmes ou policiers qui complètent l'enquête ne nient pas cet effet de déplacement mais ne sont pas en mesure de l'évaluer.
D'ailleurs, toutes les études faites à l'étranger reposent sur le même protocole de recherche : une comparaison entre une zone vidéosurveillée, une zone la jouxtant et une zone dite de contrôle présentant des caractéristiques identiques, à savoir même niveau et type de délinquance, mêmes modalités d'intervention des forces de police que celles placées sous l'œil des caméras.

A la question des taux d'élucidation dans les zones vidéosurveillées, les auteurs rapportent que dans 63 brigades de gendarmerie étudiées en 2008, 770 faits ont été élucidés grâce à la vidéosurveillance soit 12 faits par an et par brigade, soit un fait

élucidé par mois. Nonobstant ces données chiffrées, les auteurs en concluent que la vidéosurveillance apporte « *une amélioration significative du taux d'élucidation dans la majorité des communes équipées de vidéoprotection*. »

A la question de l'amélioration de la prévention et des taux d'élucidation en fonction de la densité des caméras installées, le rapport conclut à une amélioration des deux. Cependant, l'analyse du nombre de faits constatés en fonction de la densité de caméras par habitant de l'ensemble des zones étudiées ne permet pas de prouver qu'il existe un lien de causalité entre le nombre de caméras et la baisse de la délinquance constatée, les chiffres présentés dans le rapport tendant à prouver le contraire. Malgré tout, les auteurs concluent que « *l'évolution est mieux maîtrisée dans les zones ayant une densité de caméras comprise entre une caméra pour 1 000 à 2 000 habitants* » que dans celles où la densité est inférieure. Il en va de même pour le taux d'élucidation, la conclusion des auteurs selon laquelle « *le taux d'élucidation progresse plus vite dans les villes qui disposent de la densité de caméras la plus élevée* » étant fondée sur des chiffres non significatifs.

2. LE RAPPORT DE LA COUR DES COMPTES

Les seules informations fiables sont données par les rapports des chambres régionales des comptes (CRC). Ainsi, le rapport rédigé par la CRC de Rhône-Alpes en mai 2010 est explicite : « *(…) en l'état actuel des données, relier directement l'installation de la vidéosurveillance et la baisse de la délinquance est pour le moins hasardeux. Si l'on compare par exemple l'évolution de la DVP (délinquance de voie publique) entre Lyon, qui a fortement investi dans ce domaine, et Villeurbanne, où la commune n'a pas souhaité s'y engager, on observe que la baisse est plus forte dans la commune qui ne bénéficie d'aucune caméra de voie publique (…). Le dispositif de vidéosurveillance apparaît comme un outil dans l'action quotidienne de la police qui peut contribuer au maintien de la tranquillité publique. S'il peut alors apparaître réducteur de juger de la pertinence du dispositif au vu des seuls chiffres de la délinquance, on peut observer que l'outil est suffisamment coûteux (plus d'un million par an en moyenne depuis 2003, hors personnel et frais généraux liés au service) pour qu'une évaluation globale de son intérêt soit entreprise (…)* ».

Dans son rapport, la Cour des comptes[7] déplore ainsi l' « *examen rapide des dossiers* », et les « *difficultés techniques* » auxquelles les commissions sont confrontées. De plus, les magistrats soulignent que « *les risques de dérives dans l'utilisation des systèmes de vidéosurveillance sont réels, notamment en matière de respect de la vie privée* ». Ils constatent également qu' « *aucune étude d'impact, réalisée selon une méthode scientifiquement reconnue, n'a encore été publiée* », alors même que les premières villes « *vidéosurveillées* » le sont depuis le milieu des années 90, et que le gouvernement ne cesse d'en vanter les mérites.

[7] *Voir supra note 3*

3

la LÉGISLATION

A. LES TEXTES DE RÉFÉRENCES

Le cadre légal et réglementaire est dense et complexe. En effet, ce ne sont pas moins de vingt-cinq articles de lois, décrets, arrêtés et circulaires qui s'appliquent sur la vidéosurveillance.

Au fil des ans, et au gré des évolutions technologiques et des demandes de la société pour plus de sécurité, induites par les discours sur les dangers de la délinquance, du terrorisme, etc., l'Etat est passé de régulateur à promoteur ou prescripteur de vidéosurveillance.

Les premières installations de vidéosurveillance sur la voie publique l'ont été au nom du pouvoir de police générale du maire. Ce sont les débats sur les atteintes à la vie privée qui ont amené l'Etat à légiférer. La loi d'orientation et de programmation relative à la sécurité (Lops) de 1995 a, pour la première fois, introduit la distinction entre les dispositifs de vidéosurveillance situés dans des lieux ouverts au public ou non. Quant à la Loppsi 2, si elle a ramené une partie des systèmes dans le giron de la Cnil, en cas d'enregistrement des images par exemple, elle a élargi le champ d'utilisation des systèmes de vidéosurveillance et le nombre d'acteurs ayant accès aux images.

Les systèmes de vidéosurveillance peuvent relever de deux régimes juridiques que le Courrier des maires et des élus locaux de septembre 2011 tentait de résumer ainsi :
« Lorsque le dispositif de vidéoprotection est installé dans un lieu public (sur le territoire d'une commune) ou dans un lieu ouvert au public (le guichet d'une mairie), il doit être **autorisé par le préfet** *(article 10 de la loi n°95-73 du 21 janvier 1995 modifiée). Le dispositif doit faire l'objet d'une* **formalité déclarative auprès de la Cnil** *si les images sont "enregistrées ou conservées dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques". Dans un lieu privé de la collectivité (parking réservé aux agents municipaux), il doit faire l'objet d'une* **déclaration normale auprès de la Cnil***, qui doit alors préciser : la durée de conservation des images (maximum un mois) ; les destinataires des images (limités aux seules* **personnes habilitées** *en fonction de leur besoin d'en connaître).* »

LES PRINCIPAUX TEXTES

Le Code civil, dans son article 9, a trait à la protection de la vie privée. Ces dispositions sont applicables à la vidéosurveillance.
La loi du 21 janvier 1995, modifiée par l'ordonnance du 19 septembre 2000 relative à la sécurité. La loi prévoit que les systèmes de vidéosurveillance visionnant les lieux ouverts au public sont soumis à une autorisation préfectorale.

La loi du 6 août 2004, modifiant la loi du 6 janvier 1978 « Informatique et libertés ». Ce texte réglemente les systèmes de vidéosurveillance installés dans un lieu non ouvert au public, tel qu'une entreprise ou encore les systèmes implantés dans les lieux publics lorsqu'ils sont associés à une technique biométrique. C'est le cas de la reconnaissance faciale. La Cnil, dans une note rendue publique le 8 avril 2008[8], souligne que « *la concurrence de deux régimes juridiques conduit à rendre le cadre légal de la vidéosurveillance extrêmement complexe, flou et aléatoire, dans un domaine touchant aux libertés publiques fondamentales* ». Par voie de conséquence, le dispositif légal actuel devient « *source d'insécurité juridique* ».

La loi du 14 mars 2011 dite « d'orientation et de programmation de la performance de la sécurité intérieure » (Loppsi 2). Cette loi porte création d'une « Commission nationale de la vidéoprotection » qui remettra chaque année au Parlement un rapport, rendu public, rendant compte de son activité de conseil et d'évaluation de l'efficacité de la vidéoprotection. Le rapport comprend aussi les recommandations destinées au ministre de l'intérieur en ce qui concerne les caractéristiques techniques, le fonctionnement ou l'emploi des systèmes de vidéoprotection.
Pour sa part, l'article 18 de la Loppsi 2 redonne à la Cnil autorité pour les systèmes de vidéosurveillance avec enregistrements : « *Seuls sont autorisés par la Commission nationale de l'informatique et des libertés, en application de la loi n°78-17 du 6 janvier 1978 précitée, les systèmes installés sur la voie publique ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques.* »

La circulaire du 14 septembre 2011 du ministre de l'Intérieur relative au cadre juridique applicable à l'installation des caméras de vidéoprotection sur la voie publique et dans des lieux ou établissements ouverts au public, d'une part, et dans des lieux non ouverts au public, d'autre part, précise les procédures à respecter par les prescripteurs de vidéosurveillance. Cette circulaire s'appuie notamment sur l'avis du Conseil d'Etat en date du 24 mai 2011. Toutefois, pour clarifier la circulaire, la Cnil a publié sur son site au mois de juin 2012 un tableau simplifié (reproduit ci-dessous) des formalités à accomplir avant de mettre en place un système de vidéosurveillance.

[8] *Cnil, 8 avril 2008, « Vidéosurveillance et garanties des droits individuels - Note sur les difficultés d'application des règles relatives à la vidéosurveillance » - Site : www.cnil.fr*

LIEU D'INSTALLATION	AUTORISATION PREFECTORALE	DECLARATION A LA CNIL (si les images sont enregistrées)
Voie publique (rue)	⊙	
Lieux ouverts au public (commerces, banques, administrations, aéroports, gares, etc.)	⊙	
Lieux non ouverts au public dans les commerces, administrations, etc. (réserves, zones réservées au personnel, etc.)		⊙
Etablissements scolaires (abords)	⊙	
Etablissements scolaires (intérieur)		⊙
Lieux communs ouverts au public dans un immeuble d'habitation	⊙	
Lieux communs non ouverts au public dans un immeuble d'habitation		⊙
Domicile personnel	-	-
Domicile personnel avec des salariés		⊙

B. LES INSTRUMENTS JURIDIQUES INTERNATIONAUX

Le Pacte international sur les droits civils et politiques du 16 décembre 1966, dans son article 17, prévoit que « *Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance (…)* ».

La Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950 assure, dans son article 8, la protection de la vie privée.

La Convention du Conseil de l'Europe n°108/1981 du 28 janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (en cours de modernisation) englobe de facto les activités de la vidéosurveillance comportant le traitement de données à caractère personnel.

La Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000 consacre son article 7 au respect de la vie privée et familiale, et son article 8 à la protection des données à caractère personnel.

La directive 95/46/EC du 24 octobre 1995 du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. La directive est actuellement en cours de révision. Ce texte, au travers de différentes dispositions, souligne le caractère spécifique du traitement des données à caractère personnel qui inclut des sons ou des images. Ainsi, l'article 1er paragraphe 1 mentionne que « *les Etats membres assurent, conformément à la présente directive, la protection des libertés et des droits fondamentaux des personnes physiques, notamment dans leur vie privée, à l'égard du traitement des données à caractère personnel.* »

4

des LIBERTÉS à PROTÉGER

A. LES RISQUES D'ATTEINTES À LA VIE PRIVÉE

La menace principale de la multiplication des systèmes de vidéosurveillance est le traitement des données issues de ces systèmes. Les policiers et les gendarmes peuvent avoir accès aux images collectées sans le contrôle d'un juge. De leur côté, les commissions départementales de vidéosurveillance qui autorisent la mise en place des systèmes, même présidées par un magistrat, ont un fonctionnement très opaque. Quant au préfet, qui donne ou refuse les autorisations d'implantations, il est aussi chargé par l'Etat d'en faire la promotion.

Comme l'a rappelé le « Guide méthodologique de vidéoprotection » du ministère de l'Intérieur, les systèmes de vidéosurveillance, « *dans le souci de concrétiser la sûreté en sécurisant la liberté d'aller et venir* » risquent – si des précautions ne sont pas prises – « *de porter une atteinte excessive au respect de la vie privée* ». En conséquence, indiquait la Cour des comptes, « *la décision d'autoriser l'implantation d'un tel dispositif doit résulter d'une appréciation de la proportionnalité entre la réduction de l'insécurité et l'augmentation du risque d'atteinte à la vie privée résultant de chaque dispositif.* »

Force est de constater que les nouvelles techniques sont mises en œuvre avant toute analyse scientifique, indépendante de juristes ou des législateurs, sans aucune évaluation a priori de la proportionnalité entre les exigences de sécurité (réelles, supposées ou suscitées) et la protection des données personnelles et de la vie privée (reconnaissance faciale, interconnexions des fichiers d'images entre différents opérateurs, etc.).

Par ailleurs, les études montrent une tendance à la discrimination qui, si elle est involontaire, n'en est pas moins contraire à l'égalité républicaine. En effet, parmi les trop grandes quantités d'images que les opérateurs ont à surveiller, leurs choix se portent plus facilement sur les jeunes, et surtout ceux dont la tenue vestimentaire leur paraît suspecte.

Le développement rapide des technologies de vidéosurveillance, la reconnaissance faciale et les logiciels comportementalistes, voire l'utilisation de drones équipés de caméras, font craindre une surveillance de tous les instants et en tous lieux, inefficace mais généralisée, ne laissant aucune place à la vie privée dans le domaine public et obligeant le citoyen à « s'autocensurer » pour rester dans la norme.

B. LES RISQUES POUR LA SÉCURITÉ

La généralisation de ces systèmes onéreux se fait au détriment du déploiement d'une police de proximité au service des citoyens non pour répondre à des exigences réelles et objectives de sécurité mais comme remède aux carences d'organisation de la police. Les êtres humains sont remplacés par un mirage technologique normatif et destructeur de lien social. Penser que des logiciels permettront de repérer des suspects grâce à des signes distinctifs, à des comportements est une aberration intellectuelle.

La vidéosurveillance entraîne une surveillance supposée répressive par la sanction des comportements délinquants. Mais elle est surtout une surveillance préventive, et le fait d'être vu sans voir peut induire un comportement de « soumission », conformation à une « normalité » supposée, qui incite le citoyen à avoir un comportement « normal », sans que l'on sache ce que cela sous-entend.

Le pouvoir politique est devenu captif de cette technologie sécuritaire, et il n'est pas rare de rencontrer des élus qui maintiennent des systèmes obsolètes, voire des caméras hors exploitation sans le faire savoir aux administrés.

C. LE DROIT À L'INFORMATION

Même si l'espace public n'est pas le lieu où le citoyen peut s'attendre à la meilleure protection de sa vie privée, celle-ci doit être respectée. Il doit être informé de l'installation de systèmes de vidéosurveillance. En outre, le simple signalement par affichage de ces systèmes de vidéosurveillance n'est pas suffisant. Le citoyen doit savoir quelles données sont utilisées et quels sont ses droits sur l'utilisation de celles-ci.

Si la Loppsi 2 rend l'information du public obligatoire, et ceci « *de manière claire et permanente de l'existence du système de vidéosurveillance* », cette obligation n'est pas forcément respectée. Dès lors, si les caméras sont invisibles et qu'aucun panneau ne les signale, comment savoir si l'on est vidéosurveillé ?

Les autorisations des systèmes de vidéosurveillance se font la plupart du temps de façon « express » par les commissions départementales de la vidéoprotection, et ce malgré le fait que « *la décision d'autoriser l'implantation d'un tel dispositif doit résulter d'une appréciation de la proportionnalité entre la réduction de l'insécurité et l'augmentation du risque d'atteinte à la vie privée résultant de chaque dispositif* ». Dans les faits, la commission se borne à vérifier que les engagements écrits sont conformes à la réglementation. Elle ne se rend jamais sur place. Elle s'assure simplement que le formulaire de demande est correctement rempli. Bien que le respect de l'interdiction

de visionner les parties intérieures des immeubles soit censé résulter des capacités techniques des systèmes de vidéosurveillance par le biais d'un mécanisme de « floutage » ou de « flocage » sur les écrans de visualisation, aucun engagement n'est pris par écrit sur ce point.

L'information des citoyens passe également par le droit d'accès et de conservation des images. En effet, toute personne peut accéder aux enregistrements la concernant par une demande d'accès qui doit être adressée au responsable du système de vidéoprotection. Cet accès est un droit. La conservation des images est d'un mois. Par conséquent, passé ce délai, toute personne peut vérifier la destruction des images la concernant, sauf procédure judiciaire en cours.

En cas de difficulté d'accès, les personnes disposent de voies de recours :

- **la Cnil** peut, sur demande de la commission départementale des systèmes de vidéoprotection, du responsable du système ou de sa propre initiative, exercer un contrôle visant à s'assurer que le système est utilisé conformément à son autorisation et aux dispositions de la loi. Si la Cnil constate un manquement, elle peut - après mise en demeure du responsable du système de se mettre en conformité - demander au préfet d'ordonner la suspension ou la suppression du système. Elle informe le maire de la commune concernée de cette demande ;
- **la commission départementale des systèmes de vidéoprotection**. Toute personne rencontrant une difficulté dans le fonctionnement d'un système de vidéoprotection peut saisir la commission départementale. Cette instance peut aussi, en dehors de toute saisine de particuliers, décider d'exercer un contrôle des systèmes, à l'exception de la défense nationale. Enfin, elle peut émettre des recommandations, proposer la suspension ou la suppression des dispositifs non autorisés. Elle informe alors le maire de la commune de cette proposition ;
- **le juge**. Que la commission départementale ait été saisie ou non, toute personne peut également s'adresser à la juridiction compétente en cas de difficultés concernant un système de vidéoprotection. Il peut s'agir du juge administratif ou du juge judiciaire, suivant les situations et l'objet du recours, notamment qualité publique ou privée de la personne responsable du système, un recours en annulation de l'autorisation préfectorale, des poursuites pénales, etc. Le requérant peut déposer, s'il l'estime nécessaire, une demande en référé.

En tout état de cause, si un dispositif de vidéosurveillance ne respecte pas les règles posées par la loi, toute personne concernée peut saisir :
- les services des plaintes de la Cnil qui peut contrôler tous les dispositifs installés sur le territoire national, qu'ils filment les lieux ouverts ou fermés au public ;
- les services de la préfecture, si les caméras filment les abords de l'établissement ;
- les services de police ou de gendarmerie ;
- le procureur de la République.

D. LE « CONTRÔLE DES CONTRÔLEURS »

L'article 10 de la loi du 21 janvier 1995 a fait de la commission départementale une instance de contrôle de la conformité des systèmes de vidéosurveillance aux engagements pris dans les demandes d'autorisation. Il s'agit d'un avis a priori. En effet, les commissions départementales disposent de trois mois pour donner leur réponse à une demande d'installation. Leur silence vaut acceptation. Elles sont donc obligées de travailler dans l'urgence. Selon le rapport de la Cour des comptes, « *… en l'absence de moyens matériels et humains, les commissions départementales ne peuvent exercer ce pouvoir de contrôle a posteriori.* »
Ainsi, un magistrat membre d'une commission départementale a observé les limites de l'application de la loi dans les établissements vidéosurveillés : « *Dans le dossier soumis à la commission, tout était en règle (nombre de caméras, champ d'observation, lieux d'installation) mais une fois l'autorisation obtenue, des modifications peuvent être faites sans que la commission ait les moyens d'en faire le constat et même dans le cas où il serait fait, de verbaliser car elle n'en a pas les pouvoirs.* »

La Cnil, qui contrôlait jusqu'alors les seuls dispositifs de vidéosurveillance dans les lieux non-ouverts au public, est depuis la loi Loppsi 2 également compétente pour contrôler les dispositifs de vidéoprotection - pour les lieux ouverts au public et la voie publique - afin de s'assurer qu'ils sont conformes aux obligations légales. Elle peut dès lors opérer des contrôles sur les dispositifs de vidéosurveillance sur l'ensemble du territoire national à son initiative, à la demande de la commission départementale ou à la demande du responsable d'un dispositif de vidéoprotection. Près de 950 000 dispositifs sont concernés. Les principaux manquements relevés sont :
- le manque de connaissance du régime juridique applicable ;
- l'insuffisance ou l'inexistence d'information des personnes ;
- la mauvaise orientation des caméras ;
- les mesures de sécurité insuffisante.

E. L'HABILITATION DES OPÉRATEURS

En vertu de la loi du 21 janvier 1995, l'autorisation préfectorale doit prescrire « *toutes les précautions utiles, en particulier quant à la qualité des personnes chargées de l'exploitation du système de vidéosurveillance ou visionnant les images et aux mesures à prendre pour assurer le respect des dispositions de la loi* ». Les pétitionnaires doivent désigner toutes les personnes susceptibles d'accéder aux images, y compris les techniciens de maintenance.

Dans la pratique, les arrêtés préfectoraux d'autorisation ne respectent pas toujours les exigences relatives à l'identité et à la qualité des personnes chargées d'exploiter les

systèmes et de visionner les images.
Déjà en 1997, le Conseil d'Etat avait confirmé que les fonctionnaires de la police ou de la gendarmerie, d'une part, et ceux des polices municipales, d'autre part, sont les seuls à pouvoir accomplir des missions de surveillance de la voie publique. Ce principe de compétence porte sur la surveillance tant humaine que par le biais de systèmes électroniques.

Par ailleurs, par sa décision du 10 mars 2011, le Conseil constitutionnel a annulé les dispositions de l'article 18 de la Loppsi 2 qui autorisaient des personnes privées à procéder à une surveillance de la voie publique parce qu'elles constituaient « *une délégation à ces personnes de tâches inhérentes à l'exercice par l'Etat de ses missions de souveraineté* », et méconnaissaient « *les exigences constitutionnelles liées à la protection de la liberté individuelle et de la vie privée* ». C'est ainsi qu'a été retirée de la loi votée par le Parlement la possibilité pour l'autorité publique ou toute personne morale de confier par convention l'exploitation de son système de vidéosurveillance de la voie publique à un opérateur public ou privé agréé par le préfet, et le cas échéant, à une société de sécurité placée sous le régime de la loi du 12 juillet 1983 relative aux activités privées de sécurité. Il en a été de même de la disposition qui permettait à des personnes morales de droit privé de mettre en œuvre sur la voie publique un système de vidéosurveillance aux fins d'assurer la protection des abords de leurs bâtiments et installations.

F. LA CHARTE DU FORUM EUROPÉEN POUR LA SÉCURITÉ URBAINE

Le Forum européen pour la sécurité urbaine regroupe 300 collectivités locales européennes dont 130 françaises. Dans le cadre d'un projet européen sur la protection des données personnelles, le Forum européen a élaboré une « Charte pour une utilisation démocratique de la vidéosurveillance » dont les communes devraient s'inspirer lorsqu'elles ont le souhait d'installer un tel dispositif.

L'objectif de la charte est de donner aux citoyens des garanties quant à l'utilisation de ces systèmes parce que la vidéosurveillance :
- par la surveillance qu'elle exerce sur les espaces, peut être de nature à altérer l'expression des libertés individuelles dans ces espaces ;
- du fait des évolutions technologiques qui la caractérisent, est de nature à ouvrir de manière exponentielle le champ des possibles ;
- est au cœur de débats passionnés laissant émerger des inquiétudes et des craintes.
Souhaitant « replacer le citoyen au cœur des préoccupations des villes », les auteurs de la charte s'appuient sur quatre outils :
- **le diagnostic préalable** pour définir de manière objective les besoins locaux ainsi

que l'étude de la faisabilité, réalisé de préférence par un organe interne ;
- **la mise en œuvre d'évaluations périodiques**. C'est un outil d'aide à la décision pour renforcer ou modifier le système ;
- **la formation des opérateurs**. Les opérateurs de vidéosurveillance constituent la clé de voûte du système. D'eux va dépendre en partie le bon fonctionnement du système. Ces opérateurs doivent être formés aux principes fondateurs de cette charte mais également aux recommandations à mettre en œuvre. Ils doivent également intégrer les objectifs du système. La formation est une exigence de qualité ;
- **une autorité de contrôle** doit permettre de vérifier le respect des principes de la charte. L'indépendance de cette autorité doit être garantie.

La charte rappelle les principes essentiels qui doivent présider à l'installation de systèmes de vidéosurveillance :

1. **Principe de légalité** : respect de la loi et des réglementations en vigueur ;

2. **Principe de nécessité** : l'installation doit se décider à l'aune d'une nécessité soit l'adéquation entre des circonstances et un besoin d'une part, et la réponse que constitue la vidéosurveillance d'autre part.

3. **Principe de proportionnalité** : l'élaboration, l'installation, le fonctionnement et le développement des systèmes de vidéosurveillance doivent être définis par rapport à la problématique à laquelle ils doivent répondre.

4. **Principe de transparence** : nécessité d'une politique claire et lisible quant au fonctionnement du système. La transparence est très liée à la communication. Ce principe est essentiel car si la vidéosurveillance peut être considérée comme une technologie restrictive des libertés, elle doit s'accompagner d'une forte information du public.

5. **Principe de responsabilité** : les autorités en charge des systèmes de vidéosurveillance sont les garants d'une utilisation légale et respectant la vie privée et les libertés fondamentales de ces systèmes. Leur responsabilité pourra donc être engagée en cas de manquements ou de violations constatées. Les autorités administratives devant lesquelles cette responsabilité peut être mise en jeu doivent être clairement identifiées.

6. **Principe de supervision indépendante** : des freins et des contrepoids au fonctionnement des systèmes de vidéosurveillance doivent être mis en œuvre par un processus de contrôle indépendant, avec des normes définies.

7. **Principe d'implication de citoyens** : favoriser l'implication des citoyens à toutes les étapes à travers différentes formes de consultation, de participation, de délibération et de codécision.

En France, cette charte a été signée, notamment, par les villes de Saint-Herblain, Echirolles et Toulouse.

CONCLUSION

En 2004 le Livre bleu, écrit pour la présentation prospective du Groupement professionnel des industries de composants et de systèmes électroniques (GiXel), posait le problème de l'acceptabilité par la population de ces dispositifs : « *La sécurité est très souvent vécue dans nos sociétés démocratiques comme une atteinte aux libertés individuelles. Il faut donc faire accepter par la population les technologies utilisées et parmi celles-ci la biométrie, la vidéosurveillance et les contrôles* ».
Si le GiXel avait des solutions pour la biométrie, passant notamment par la convivialité, il constatait : « *La même approche ne peut pas être prise pour faire accepter les technologies de surveillance et de contrôle, il faudra probablement recourir à la persuasion et à la réglementation en démontrant l'apport de ces technologies à la sérénité de la population et en minimisant la gêne occasionnée. Là encore, l'électronique et l'informatique peuvent contribuer largement à cette tâche.* »

Ce texte démontre le peu d'importance que le lobby « industrio-financier » accorde aux libertés et aux droits fondamentaux dans notre pays. Cette constatation ajoutée à la détermination de l'Etat de vouloir tout savoir sur ses concitoyens qu'il considère comme potentiellement dangereux, tricheurs et fraudeurs, est la démonstration que nous sommes entrés dans une société de surveillance généralisée.

Le développement de la surveillance, du fichage et du traçage policiers – pour mémoire, 36 fichiers en 2006, plus de 80 aujourd'hui, et plus de 42 loi sécuritaires en 10 ans – en est une preuve complémentaire.

ANNEXES

Sites Internet

- Le site de la Commission nationale informatique et libertés (Cnil) :

http://www.cnil.fr/dossiers/videosurveillance/

http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil/declaration-videosurveillance/

http://www.cnil.fr/nc/la-cnil/actualite/article/article/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de/

- Le site du ministère de l'Intérieur britannique donne accès aux différents rapports d'évaluation d'impact :

http://www.homeoffice.gov.uk/rds/cctv2.html

- Conseil de l'Europe, Commission de Venise - Commission européenne pour la démocratie par le droit – « Avis sur la vidéosurveillance dans les lieux publics par les autorités publiques et la protection des droits de l'Homme », 2007 :

http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-f.pdf

- Rapport de la Cour nationale des comptes 2011 :

http://www.ccomptes.fr/fr/Publications/Publications/Organisation-et-gestion-des-forces-de-securite-publique

- Blogs proposant différents articles sur la vidéosurveillance :

http://owni.fr/

http://bugbrother.blog.lemonde.fr/2012/10/14/indect-et-le-rideau-de-fer-securitaire-europeen/#more-3737

http://www.emilietherouin.fr/evaluation-de-la-videosurveillance-amiens-vers-une-communication-des-conclusions-en-septembre/

http://blog.mondediplo.net/2012-02-23-La-videosurveillance-se-cherche-un-alibi

http://www.laurent-mucchielli.org/index.php?post/2010/04/30/Vid%C3%A9osurveillance-%3A-le-dossier

Bibliographie

Vidéosurveillance ou vidéoprotection ? Eric Heilmann et Philippe Melchior, Editions Le Muscadier, juin 2012.

Vidéosurveillance et vidéoprotection, Alain Bauer et François Freynetn Edition Le Muscadier, juin 2012.

Filmer, ficher, enfermer, Vers une société de surveillance, coordination Evelyne Sire-Marin, Editions Syllepse, décembre 2010.

Une société de surveillance ? Etat des droits de l'Homme en France (Edition 2009), Ligue des droits de l'Homme, Editions la Découverte, avril 2009.

DANS LA COLLECTION DES GUIDES JURIDIQUES DE LA LDH

- Contre les discriminations
- La protection des données personnelles

La LDH...

Lors de la création de la Ligue des droits de l'Homme en 1898 à la suite de l'Affaire Dreyfus, le manifeste des fondateurs assurait : « ***A partir de ce jour, toute personne dont la liberté serait menacée ou dont le droit serait violé est assurée de trouver auprès de nous aide et assistance*** *». Depuis plus de cent ans, cet engagement a soutenu l'action de la LDH, que ce soit pour lutter contre l'antisémitisme, le racisme et toutes les discriminations, ou pour la défense des étrangers et le soutien à toutes les victimes d'injustices.*

Dès sa création la LDH a eu la volonté de lutter contre « ***toutes les formes d'intolérance et d'arbitraire*** *», ce qui l'a amenée à découvrir sans cesse de nouvelles injustices, de nouvelles menaces pour les libertés comme celles qui pèsent de nos jours sur la vie privée (surveillance liée aux Tic). Elle s'est attachée notamment à la défense de la laïcité contre tous les intégrismes, des droits économiques, sociaux et culturels, du droit au logement et à l'accès aux soins pour tous, et de l'égalité femmes-hommes.*

Pas de démocratie sans contre-pouvoirs *: c'est de là que découle son rôle d'****interpellation****, dans un souci d'****indépendance*** *à l'égard de tous les pouvoirs. Contre-pouvoir, la LDH l'est aussi par sa capacité de* ***rassemblement*** *: persuadée que* ***les droits de l'Homme ne sont vraiment respectés que si les citoyens s'en emparent et agissent ensemble****, elle se veut un lieu ouvert et pluraliste où peuvent se retrouver toutes celles et ceux qui souhaitent débattre et agir pour les droits de l'Homme et la citoyenneté.*

...et la LDH c'est aussi...

DES PUBLICATIONS :

- ***Etat des droits de l'Homme en France*** *(Edition 2012)* Un autre avenir ?
- ***Ceux qui nous veulent du bien*** *17 mauvaises nouvelles d'un futur bien géré.*
- ***Sous surveillance*** *- Bande dessinée*
- **Hors-série *Hommes & Libertés*** *Tous surveillés, tous surveillants ?*

UNE REVUE : ***Hommes & Libertés***

UNE PERMANENCE JURIDIQUE :
Tél : 01 56 55 50 10
(du lundi au vendredi de 10h à 13h)

UN SITE WEB : www.ldh-france.org

UNE PAGE FACEBOOK : www.facebook.com/pages/Ligue-des-Droits-de-lHomme/91187778160?fref=ts

UNE BOUTIQUE :
Tél : 01 56 55 51 04
laboutique@ldh-france.org