N° 131

SÉNAT

SESSION ORDINAIRE DE 2008-2009

Annexe au procès-verbal de la séance du 10 décembre 2008

RAPPORT D'INFORMATION

FAIT

au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par le groupe de travail (2) sur la **vidéosurveillance***,*

Par MM. Jean-Patrick COURTOIS et Charles GAUTIER,

Sénateurs.

(1) Cette commission est composée de : M. Jean-Jacques Hyest*, président ;* M. Nicolas Alfonsi, Mme Nicole Borvo Cohen-Seat, MM. Patrice Gélard, Jean-René Lecerf, Jean-Claude Peyronnet, Jean-Pierre Sueur, Mme Catherine Troendle, M. François Zocchetto*, vice-présidents ;* MM. Laurent Béteille, Christian Cointat, Charles Gautier, Jacques Mahéas*, secrétaires ;* M. Alain Anziani, Mmes Éliane Assassi, Nicole Bonnefoy, Alima Boumediene-Thiery, MM. Elie Brun, François-Noël Buffet, Pierre-Yves Collombat, Jean-Patrick Courtois, Mme Marie-Hélène Des Esgaulx, M. Yves Détraigne, Mme Anne-Marie Escoffier, MM. Pierre Fauchon, Louis-Constant Fleming, Gaston Flosse, Christophe-André Frassa, Bernard Frimat, René Garrec, Jean-Claude Gaudin, Mmes Jacqueline Gourault, Virginie Klès, MM. Antoine Lefèvre, Dominique de Legge, Mme Josiane Mathon-Poinat, MM. Jacques Mézard, Jean-Pierre Michel, François Pillet, Hugues Portelli, Roland Povinelli, Bernard Saugey, Simon Sutour, Richard Tuheiava, Alex Türk, Jean-Pierre Vial, Jean-Paul Virapoullé, Richard Yung.

(2) Ce groupe de travail est composé de : MM. Jean-Patrick Courtois et Charles Gautier

S O M M A I R E

Pages

LES ONZE RECOMMANDATIONS DU GROUPE DE TRAVAIL

Recommandation n°1 - Réunir sous une seule autorité, la CNIL, les compétences d'autorisation et de contrôle en matière de vidéosurveillance.

MIEUX PROTÉGER ET INFORMER LE PUBLIC

Recommandation n° 2 - Mieux notifier les sites au public :

- par une signalisation effective sur la voie publique ;
- par la mise en ligne de cartes indiquant les zones de la voie publique placées sous vidéosurveillance ;
- par la présentation chaque année d'un rapport d'activité de l'ensemble des systèmes de vidéosurveillance au conseil municipal ou au conseil communautaire ;
- par la mention de la durée de conservation des images sur les panneaux signalant un système de vidéosurveillance.

Recommandation n° 3 - Ne pas déléguer la vidéosurveillance de la voie publique à des personnes privées, ni permettre aux autorités publiques de vendre des prestations de vidéosurveillance de la voie publique à des personnes privées.

Recommandation n° 4 - Former, professionnaliser et habiliter les opérateurs chargés de visionner les images de la voie publique.

Recommandation n° 5 - Ne pas interdire a priori les systèmes de vidéosurveillance « intelligente », mais les soumettre à des conditions plus strictes sous le contrôle de la CNIL.

CRÉER LES CONDITIONS D'UN SYSTÈME DE VIDÉOSURVEILLANCE EFFICACE

Recommandation n° 6 – Un usage raisonné de la vidéosurveillance doit être favorisé, l'accent devant porter sur la qualité des systèmes plutôt que sur la multiplication du nombre de caméras implantées. Cela suppose en particulier :

- une phase de conception longue et approfondie ;

- des partenariats très étroits entre tous les acteurs : collectivités, services de police et de gendarmerie, commerçants, bailleurs sociaux, transporteurs… Toutefois, ce partenariat ne signifie pas la confusion des rôles, chacun devant rester dans son champ de compétence ;

- une formation de tous les acteurs pour acquérir le réflexe d'utiliser la vidéosurveillance et apprendre à l'utiliser ;

- le développement des systèmes de vidéosurveillance au niveau des bassins de vie. A cet égard, cette compétence devrait être transférée automatiquement aux établissements publics de coopération intercommunale qui exercent déjà la compétence relative à la prévention de la délinquance.

SIMPLIFIER LES PROCÉDURES ET S'ADAPTER À DE NOUVELLES UTILISATIONS

Recommandation n° 7 – Différencier le traitement administratif des demandes d'autorisation en fonction de la taille et de la nature des systèmes de vidéosurveillance. Une procédure simplifiée pourrait s'appliquer aux systèmes les plus simples dans les lieux ouverts au public.

Recommandation n° 8 - Plutôt que de délivrer une autorisation pour chaque caméra installée, des zones vidéo surveillées devraient être délimitées à l'intérieur desquelles le responsable du système de vidéosurveillance serait libre de déplacer les caméras et d'en moduler le nombre dans la limite d'un plafond.

Recommandation n° 9 – Soumettre à une procédure simplifiée les dossiers de renouvellement des autorisations, sauf en cas de modification substantielle.

Recommandation n° 10 – Admettre d'autres finalités pour l'utilisation de la vidéosurveillance à la condition que ces finalités restent accessoires par rapport aux finalités principales que sont la prévention de la délinquance, la protection des bâtiments et la régulation du trafic routier.

Recommandation n° 11 – Faciliter le recours à des dispositifs mobiles de vidéosurveillance implantés pour une durée limitée, par exemple à l'occasion d'une manifestation ou d'un évènement culturel ou sportif présentant des risques particuliers de délinquance, de préférence à des dispositifs permanents à l'utilité variable.

Mesdames, messieurs,

Au cours de sa réunion du 16 avril 2008, la commission des lois a décidé la création d'un groupe de travail sur la vidéosurveillance composé de vos deux co-rapporteurs.

La création de ce groupe de travail faisait suite à l'audition par la commission des lois de M. Alex Türk[1], président de la Commission nationale informatique et libertés (CNIL), et de M. Alain Bauer[2], président de la commission nationale de la vidéosurveillance.

Ces auditions avaient fait apparaître des incertitudes sur le régime juridique et la pertinence de la vidéosurveillance au moment où celle-ci connaît un développement accéléré sous le double effet des innovations technologiques, de l'impulsion de l'Etat et des élus locaux.

Les travaux de vos co-rapporteurs –outre de nombreuses auditions, des déplacements ont été effectués au siège de la RATP, au Technocentre d'Orange et à Londres- se sont nourris des réflexions menées simultanément par diverses instances sur ce thème.

En effet, sur les bases d'un rapport commandé à M. Philippe Melchior, inspecteur général de l'administration, le ministère de l'intérieur a lancé en novembre 2007 un plan de développement de la vidéosurveillance se fixant comme objectif de tripler le nombre de caméras en 2009.

Par ailleurs, l'Institut national des hautes études de sécurité (INHES) a publié en mai 2008 un rapport sur les conditions d'efficacité et les critères d'évaluation de la vidéosurveillance[3].

Enfin, la CNIL a publié plusieurs documents faisant le point sur les difficultés d'interprétation de la loi du 21 janvier 1995 d'orientation et de programmation pour la sécurité[4].

---

[1] *Le 3 octobre 2007.*
[2] *Le 9 avril 2008.*
[3] *http://www.inhes.interieur.gouv.fr/fichiers/rapportvideoprotectionjuillet2008.pdf.*
[4] *http://www.cnil.fr/index.php?id=2413&news[uid]=531&cHash=c82d9a732e.*

Comme l'écrit M. Frédéric Ocqueteau, chercheur au CNRS,[1] les techniques privées de surveillance à distance, au rang desquelles figure la vidéosurveillance, sont un exemple « *de la façon dont logiques techniques et logiques sociales s'articulent avec les logiques d'offre (elles-mêmes guidées par les prescriptions normatives d'un Etat arbitre devant concilier liberté et sécurité), et les logiques d'usage* ».

Cette grille d'analyse peut être utilement retenue pour l'étude de la vidéosurveillance en France et de ses évolutions depuis le début des années 90.

Techniquement, les systèmes de vidéosurveillance ont beaucoup progressé et les prochaines années devraient être celles de la « vidéo-intelligente » et de la biométrie.

Parallèlement, l'attitude générale est passée de la méfiance à une demande de vidéosurveillance, à tel point que certains emploient désormais le terme de vidéoprotection. L'Etat qui était longtemps resté en retrait, jouant un rôle d'arbitre, est ainsi devenu le principal promoteur de cette technologie au service de sa politique de sécurité.

Économiquement, la vidéosurveillance est désormais un marché mature sur lequel des acteurs non spécialisés comme les opérateurs de télécommunication commencent à entrer.

Enfin, les utilisations sont de plus en plus variées, même si l'Etat tend à orienter selon sa logique propre les systèmes de vidéosurveillance vers des finalités de sécurité.

En quinze ans, le paysage de la vidéosurveillance a donc profondément changé.

Toutefois, paradoxalement, la question de l'efficacité de la vidéosurveillance qui devrait pourtant être un préalable nécessaire n'a toujours pas été tranchée. Si au début les polémiques relatives à la vidéosurveillance opposaient les partisans de la sécurité et les défenseurs des libertés, les débats actuels mettent aux prises les convaincus et les circonspects sur son efficacité.

Force est de reconnaître que les études disponibles ne permettent pas de se prononcer aisément. Le rapport précité de l'INHES donne d'ailleurs assez peu de données statistiques pour évaluer l'efficacité de la vidéosurveillance. Il ouvre surtout des pistes pour mener à l'avenir des études pertinentes et fiables.

Enfin, il faut observer que le cadre juridique de la vidéosurveillance a peu évolué depuis 1995. Vos co-rapporteurs se sont particulièrement attachés à savoir si ce cadre juridique était encore adapté et de nature, au-delà des apparences de la procédure d'autorisation, à protéger les libertés individuelles et le respect de la vie privée.

---

[1] *In « Polices entre Etat et marché » aux éditions Presses de la Fondation nationale des sciences politiques (2004), page 114.*

I. L'ÂGE DE LA MATURITÉ DE LA VIDÉOSURVEILLANCE

A. UNE TECHNOLOGIE DE MIEUX EN MIEUX ACCEPTÉE

1. Un outil qui a suscité de vifs débats à ses débuts et de nombreuses inquiétudes

Les premiers dispositifs de vidéosurveillance se sont développés au cours des années 80 et au début des années 90, principalement dans les espaces commerciaux et privés. Toutefois, les autorités publiques -Etat et collectivités territoriales- y avaient également recours pour la surveillance de bâtiments publics ou du trafic automobile.

Les réflexions et les débats sur le cadre légal de la vidéosurveillance et sur les risques pour les libertés collectives et individuelles ont réellement émergé lorsque certaines communes ont souhaité mettre en place des réseaux de vidéosurveillance de la voie publique en tant que telle aux fins de prévenir et réprimer la délinquance.

Le premier cas fut celui d'Avignon. Le 21 juin 1990, le tribunal administratif de Marseille annula la décision de la ville d'installer 98 caméras de surveillance et un poste central, placés sous le contrôle de la police nationale. Il avait estimé que « *l'installation généralisée et le fonctionnement permanent de caméras portait une atteinte excessive aux libertés individuelles et notamment au droit à la vie privée et à l'image qui n'était justifiée ni par une habilitation judiciaire, ni par les nécessités de l'ordre public ou la constatation ponctuelle d'infractions au code de la route ou d'atteintes aux biens ou aux personnes* ».

Mais l'exemple le plus médiatique fut celui de la ville de Levallois-Perret (Hauts-de-Seine) qui décida quelques années plus tard de déployer un réseau complet de caméras.

Compte tenu de la polémique et du flou entourant le régime légal de la vidéosurveillance sur la voie publique, la CNIL fut saisie pour avis. Celle-ci se déclara incompétente mais souligna que « *le procédé de surveillance des voies et places publiques par le moyen de caméras* » était dans son principe « *de nature à constituer un risque pour les libertés et principalement celle, fondamentale et constitutionnelle, d'aller et venir* » et qu'il pouvait « *également occasionner des atteintes à la vie privée* »[1]. En revanche, le juge administratif ne fut pas saisi d'un recours à l'inverse de l'exemple d'Avignon.

Ces projets et leur mise en oeuvre dans le cas de Levallois-Perret cristallisèrent des oppositions très fortes que l'adoption de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (LOPS) fixant le régime légal de la vidéosurveillance sur la voie publique et dans les lieux ouverts au public ne permit de réduire que progressivement.

---

[1] *Délibération n°93-001 du 12 janvier 1993.*

2. Un débat apaisé

Vos rapporteurs ont systématiquement demandé aux personnes entendues si elles avaient eu connaissance de dérapages ou d'utilisations abusives de la vidéosurveillance, qui auraient en particulier porté atteinte au respect de la vie privée. Or, aucune utilisation manifestement abusive ne semble avoir été constatée dans les espaces publics. En revanche, il est par définition moins aisé de se prononcer sur le cas des caméras qui n'ont pas à être autorisés, car se trouvant dans des lieux non ouverts au public et dont le nombre est très élevé.

M. Frédéric Ocqueteau, chercheur au CNRS et professeur à Paris II, a indiqué que les débats sur la vidéosurveillance « instrument liberticide », qui avaient entouré l'installation des premiers systèmes sur la voie publique au début des années 90, avaient cédé la place dix années plus tard à un débat sur les conditions d'un bon usage de la vidéosurveillance.

Il a relevé que la dramatisation de l'époque était largement retombée. Un indice est par exemple le très faible nombre de demandes de consultation des images de la part de personnes craignant une atteinte à leur vie privée.

Cet apaisement apparent du débat se traduit aussi par l'absence de clivage entre les communes selon leur orientation politique. Des maires de toute sensibilité politique ont choisi de doter leur commune d'un système de vidéosurveillance. C'est ainsi que 100 % des communes de plus de 100.000 habitants en sont désormais équipées.

Dans un récent sondage confié à IPSOS par la CNIL[1], 71 % des sondés se déclaraient favorables à la présence de caméras de vidéosurveillance dans les lieux publics. Cette transformation de la perception de cette technologie se traduit également dans la terminologie utilisée, le ministère de l'intérieur parlant désormais de vidéoprotection et non de vidéosurveillance.

De manière générale, l'image filmée de notre vie quotidienne s'est également banalisée avec la multiplication des caméras dans les espaces privées, les établissements recevant du public ou au domicile des particuliers avec les caméras de surveillance et les webcams. Enfin, même si cela ne relève pas de la vidéosurveillance, il est probable que l'apparition de la télé-réalité et le développement des blogs ont modifié la frontière entre vie privée et vie publique.

3. Un débat qui reste d'actualité

Dans ce contexte, les enjeux de libertés publiques et individuelles apparaissent moins porter sur l'outil vidéosurveillance lui-même que sur les possibilités de le combiner avec d'autres technologies de surveillance ou de détection comme la biométrie.

---

[1] *Etude réalisée en face-à-face du 14 au 17 mars 2008 auprès d'un échantillon de 972 personnes, représentatives de la population française âgée de 18 ans et plus.*

Les craintes relatives à une utilisation liberticide de la vidéosurveillance au début des années 90 étaient très fortes. Pourtant, d'une certaine façon, elles étaient exagérées ou prématurées compte tenu de la technologie de l'époque : image de mauvaise qualité, défaillances nombreuses, capacité d'enregistrement limitée… De fait, ces limites techniques faisaient que la plupart des systèmes de vidéosurveillance de la voie publique était plutôt utilisée pour surveiller le trafic routier que pour prévenir ou réprimer la délinquance.

A l'inverse, aujourd'hui, ces craintes ont perdu de leur intensité alors que les progrès technologiques autorisent ou vont autoriser des utilisations potentiellement beaucoup plus intrusives sur le plan du respect de la vie privée et des libertés.

En outre, l'absence de scandale lié à un détournement d'un système de vidéosurveillance à des fins illégales ne signifie pas que tous les systèmes installés sont en conformité avec la loi.

La CNIL est ainsi saisie chaque année de plaintes (114 en 2006 et 121 en 2007), pour la plupart dans des lieux non ouverts au public (bureaux, copropriétés…).

S'agissant des systèmes de vidéosurveillance dans les espaces publics, si en moyenne seulement une petite vingtaine de plaintes est adressée chaque année aux préfets, en revanche les contrôles des commissions départementales de vidéosurveillance, pourtant limités, donnent lieu à la constatation d'un nombre significatif d'infractions.

En 2006, sur 869 contrôles, 22 % ont fait apparaître des infractions. En 2007, sur 483 contrôles, ce même taux était de 11 %.

M. Philippe Melchior, président du Comité de pilotage stratégique de la vidéosurveillance, a aussi indiqué que des systèmes de vidéosurveillance relevant de la loi du 21 janvier 1995 étaient installés **sans autorisation**, leur responsable déclarant parfois avoir été découragé par la lenteur des procédures…

B. DES TECHNOLOGIES DE PLUS EN PLUS PERFORMANTES POUR DES UTILISATIONS TOUJOURS PLUS VARIÉES

Les premiers systèmes de vidéosurveillance étaient des systèmes analogiques. Désormais, l'intégralité des nouveaux systèmes sont des systèmes numériques. Le stock de l'analogique est difficile à évaluer, mais il tend à devenir de plus en plus résiduel compte tenu de ses défauts.

Le passage de l'analogique au numérique a permis d'augmenter la puissance des objectifs et les capacités de mémorisation, de stockage et de consultation des images.

1. Une technologie qui se combine à d'autres

La vidéosurveillance fut initialement utilisée seule. Elle tend toutefois à se combiner de plus en plus avec d'autres techniques, même si certaines doivent être encore améliorées.

Une première possibilité, déjà ancienne mais sans cesse perfectionnée, est l'association de la vidéosurveillance à un capteur de mouvement ou à une alarme. L'opérateur est alors alerté ou l'enregistrement de l'image se déclenche.

Un autre cas est **l'association du son et de l'image**, en continu ou ponctuellement. Elle est déjà utilisée sur de nombreux réseaux de bus, notamment à la RATP. Les sons à proximité du chauffeur sont notamment enregistrés afin de mieux comprendre, a posteriori, les causes et le déroulement d'un incident. Lors de son audition, Mme Sophie Vuillet-Tavernier, directrice des affaires juridiques, internationales et de l'expertise à la CNIL, a souligné le développement de cette fonctionnalité supplémentaire, tout en s'interrogeant sur sa compatibilité avec la LOPS du 21 janvier 1995 qui n'envisage pas ce cas de figure. L'arrêté du 26 septembre 2006 fixant des normes techniques minimales pour les systèmes de vidéosurveillance ne comporte aucune précision sur ce point.

L'utilisation de la géolocalisation par GPS tend également à se développer, notamment pour améliorer les délais d'intervention en cas de détection d'un incident ou d'un évènement anormal. A Londres, les agents de police en service sont géolocalisés, ce qui permet de mobiliser rapidement les agents les plus proches.

D'autres solutions sont en cours de développement. Toutefois, de l'avis de toutes les personnes entendues, leur manque de fiabilité constitue pour le moment un obstacle à leur exploitation en conditions réelles.

Il s'agit notamment de la mise au point de systèmes de vidéosurveillance « intelligents » capables de détecter, par exemple dans une foule, des mouvements ou des sons anormaux (une personne qui court, des cris…).

Le second axe de recherche est **la biométrie**, et en particulier la reconnaissance faciale. En théorie, il serait possible d'identifier une personne dans une foule. Des expérimentations ont été lancées dans certains aéroports et gares britanniques, mais le taux d'erreur est très important. Si l'ensemble des industriels travaillent sur cette technologie, il est impossible de prédire à quel horizon une offre technique pourra être proposée à des utilisateurs. En revanche, il est probable que lorsqu'elle le sera, elle recevra des applications dans les gares internationales ou les aéroports. M. Frédéric Péchenard, directeur général de la police nationale, a d'ailleurs évoqué les réflexions actuelles sur la constitution d'un fichier « photos » sur le modèle du fichier national automatisé des empreintes génétiques (FNAEG) qui permettrait de

reconstituer un visage[1] et de le comparer avec des enregistrements sur une scène d'infraction. Un projet similaire a démarré au Royaume-Uni avant d'être interrompu pour des raisons éthiques et techniques, la crainte d'une partie de l'opinion étant que ce fichier puisse être interconnecté avec l'éventuel fichier national de la carte nationale d'identité.

Cette perspective changerait considérablement la nature de l'outil. Les craintes quant à une société de surveillance seraient considérablement ravivées et justifiées. On peut d'ailleurs se demander si ce type d'application ne remettrait pas en cause l'acceptation de la vidéoprotection par les citoyens. A cet égard, le terme de vidéosurveillance redeviendrait mieux approprié.

Toutefois, il faut être conscient que notre législation ouvre d'une certaine manière la voie à ce type d'utilisation.

Ainsi, l'article 78-2 du code de procédure pénale autorise **sans conditions** les contrôles physiques d'identité dans les zones accessibles au public des ports, aéroports et gares ouverts au trafic international et désignés par arrêté. Néanmoins, ces contrôles ne se font pas à l'insu de la personne.

Surtout, le système de lecture automatisée des plaques d'immatriculation (LAPI- voir ci-dessous) est d'une nature assez proche, même s'il ne s'appuie pas sur la biométrie. Il s'agit cette fois d'un contrôle systématique et à l'insu des personnes.

A la suite de la visite du Technocentre Orange, vos co-rapporteurs attirent également l'attention sur **les développements liés à l'Internet.**

Les grands opérateurs de télécommunication disposent en effet d'un réseau IP sur l'ensemble du territoire. Grâce à la numérisation, toutes sortes de données (images, sons…) peuvent être transmises sur ce réseau, puis stockées à distance. **La vidéosurveillance ne serait qu'une application parmi d'autres**.

Cette offre technique et commerciale présente plusieurs avantages.

Premier avantage, la commune ou tout autre utilisateur de la vidéosurveillance n'a pas à déployer un réseau vidéo dédié. Il suffit de brancher les caméras sur le réseau IP. L'économie en résultant est importante, puisqu'en investissement, le déploiement du réseau et les travaux afférant (terrassement…) représente généralement le principal poste de dépense.

Second avantage, l'opérateur de télécommunication[2] peut prendre en charge le stockage des images, celles-ci pouvant être consultées à distance de n'importe quel endroit pourvu que la personne y soit autorisée. On peut ainsi imaginer que des policiers ou des gendarmes puissent pour les besoins d'une enquête ou en cas d'évènements graves visionner des images sans avoir à se déplacer dans les locaux de la police municipale, d'un centre commercial ou du commissariat local.

---

[1] *Une simple photo ne suffit pas. Le visage est pris sous plusieurs angles.*

[2] *L'habilitation de l'opérateur n'est pas indispensable. En revanche, ce mode d'enregistrement et de conservation des images doit être mentionné dans l'autorisation, après que des garanties ont été données sur la protection des enregistrements par l'opérateur.*

Ces différentes évolutions technologiques sont appelées à modifier profondément l'utilisation de la vidéosurveillance dans les prochaines années.

2. Des utilisations très variées, des plus rudimentaires aux plus innovantes

Le spectre des modes d'utilisation de la vidéosurveillance n'a cessé de s'élargir.

Les utilisations classiques sur site fixe (retransmission sur un moniteur sans enregistrement, enregistrement sans retransmission en temps réel, visionnage en temps réel avec enregistrement) se sont perfectionnées, mais elles n'ont pas réellement changé.

En revanche, depuis quelques années, on constate le développement de la vidéosurveillance mobile[1].

Ainsi, afin de sécuriser les policiers et gendarmes et de fournir à l'autorité judiciaire des précisions sur les conditions d'une interpellation, de plus en plus de véhicules des forces de l'ordre sont équipés de **caméras embarquées.**

Dans la police nationale, de nombreux véhicules sont désormais équipés, en particulier ceux des brigades anti-criminalité. En Seine-Saint-Denis par exemple, la plupart des véhicules sont désormais équipés de caméras embarquées.

Le général Guy Parayre, ancien directeur général de la gendarmerie nationale, a indiqué que 450 véhicules de gendarmerie devraient en être équipés pour un montant de 5 millions d'euros dans le cadre de la future loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI). De même, neuf hélicoptères en seront aussi équipés.

Toutefois, il a concédé que le fondement juridique de ces caméras embarquées manquait, la LOPS du 21 janvier 1995 n'ayant envisagé que des caméras fixes. Il a d'ailleurs cité le cas d'un préfet ayant refusé d'autoriser de tels dispositifs dans un département. En revanche, M. Frédéric Péchenard, directeur général de la police nationale, a déclaré ne pas avoir rencontré ce type de difficultés juridiques[2].

La course à la miniaturisation ouvre d'autres possibilités encore.

D'ores et déjà, les TASER sont équipés de caméras et d'un micro.

Surtout, des policiers et gendarmes devraient prochainement être équipés de caméras qui seraient fixées sur leur uniforme. Si la stabilité de l'image n'était pas encore satisfaisante, les avancées de la recherche permettent désormais de déployer ces dispositifs. Vos rapporteurs ont d'ailleurs constaté que des policiers britanniques en étaient désormais dotés.

---

[1] *L'essor de la vidéosurveillance dans les transports en commun, dans les bus en particulier, n'en relève pas car le plan reste fixe même si le support –le véhicule- est mobile.*

[2] *Sur cette difficulté, voir le II.C.3.*

Si les images de ces caméras embarquées sont aujourd'hui utilisées a posteriori, il est probable qu'elles seront prochainement renvoyées directement vers un poste de commandement qui pourra, s'il en a besoin, les visionner en temps réel.

Une autre évolution majeure est l'utilisation de la vidéosurveillance à des fins d'identification automatique et systématique.

En France, les premières expérimentations du **système de lecture automatisée des plaques d'immatriculation (LAPI)**[1] ont été lancées en 2007. Plus de 400.000 plaques d'immatriculation ont été lues en l'espace de ces quelques mois d'expérimentation.

Dans la gendarmerie, un dispositif est actuellement expérimenté en Haute-Garonne. Le général Guy Parayre a indiqué que son objectif était de se doter à terme d'au moins une centaine de ces dispositifs. Dans le cadre de la LOPPSI, 3,1 millions d'euros y seront consacrés[2].

Dans la police nationale, deux véhicules en sont équipés ; quatre autres devraient l'être avant la fin de l'année 2008.

L'expérimentation actuelle doit être complétée par des dispositifs fixes en plusieurs points du territoire, notamment sur les points d'entrée très fréquentés de Paris. Le ministère de l'intérieur étudierait également la possibilité de coupler ce nouveau dispositif avec certains des radars automatisés mis en place depuis 2003 afin de lutter contre la vitesse excessive au volant.

---

[1] L'article 8 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme a consolidé le système de surveillance automatique des véhicules que la loi du 18 mars 2003 pour la sécurité intérieure avait déjà autorisé, sans qu'il ait jamais été mis en œuvre.
Ce système de lecture automatisé des plaques d'immatriculation (LAPI) fait donc l'objet de dispositions légales propres. Compte tenu de ses spécificités, il ne pouvait pas relever de la législation relative à la vidéosurveillance.
Il permet d'enregistrer et de comparer avec le fichier des véhicules volés et signalés (FVV) l'ensemble des véhicules passant à un endroit. Les finalités sont très larges : délits douaniers, lutte contre la criminalité, le terrorisme…Outre la plaque d'immatriculation, la photographie des passagers est également enregistrée. Les données ainsi collectées sont conservées huit jours maximum, sauf en cas de rapprochement avec le FVV. Les dispositifs peuvent être fixes ou mobiles, notamment à l'occasion d'évènements ponctuels comme des grands rassemblements.

[2] Il convient de relever que le Parlement a été conduit à discuter, dans le cadre de l'examen du projet de loi de finances pour 2009, de la première année d'exécution budgétaire d'une loi, la LOPPSI, qui n'a toujours pas été adoptée en conseil des ministres. Ce texte doit préciser les moyens financiers en appui à des moyens juridiques. Toutefois, le Parlement ne peut à ce jour en mesurer concrètement la portée.

C. L'ESSOR DE LA VIDEOSURVEILLANCE

Après une phase de démarrage de la vidéosurveillance relativement lente, en raison notamment des craintes de l'opinion quant au respect des libertés individuelles et de la vie privée, on assiste à un basculement avec l'émergence d'une demande forte en faveur de la vidéosurveillance. Certains élus se trouvent même en retrait par rapport aux demandes de la population. Cet essor de la vidéosurveillance est accéléré par la nouvelle stratégie de l'Etat qui s'était tenu en retrait jusqu'en 2007.

1. Des estimations approximatives

Selon M. Philippe Melchior, responsable du Comité de pilotage stratégique de la vidéosurveillance et auteur de plusieurs rapports sur ce thème pour le compte du ministère de l'intérieur, environ 350.000 caméras ont fait l'objet d'une autorisation conformément à l'article 10 de la LOPS du 21 janvier 1995. Il s'agit uniquement des caméras sur la voie publique ou dans les lieux ouverts au public. On notera que selon le ministère de l'intérieur, le nombre de caméras autorisées s'élevait à 396.000 à la fin de l'année 2007.

Elles se répartissent approximativement de la façon suivante :

- 80 % dans des établissements privés recevant du public ;

- 14 % dans les transports ;

- 6 % (20.000 caméras environ) sur la voie publique.

Ces données sont toutefois à prendre avec précaution. Certains systèmes sont sans doute installés sans autorisation et peuvent faire l'objet de régularisation a posteriori. En sens contraire, des autorisations sont accordées, mais les caméras ne sont pas nécessairement installées.

S'agissant des 20.000 caméras autorisées sur la voie publique, il a jugé le nombre de 12.000 installées plus proche de la réalité.

2. Une hausse importante du nombre de systèmes autorisés, en particulier sur la voie publique

On observe une accélération du déploiement de la vidéosurveillance depuis plusieurs années.

Évolution du nombre d'autorisations délivrées en application de la loi du 21 janvier 1995

	1997-1998	1999	2000	2001	2002
Nombre d'autorisations délivrées	34.269* dont 4.985 nouveaux systèmes	4.681 (- 6 %)	3.607 (- 23 %)	4.511 (+ 25 %)	4.977 (+ 10 %)

* période de régularisation des systèmes installés antérieurement à l'entrée en vigueur de la réglementation

	2003	2004	2005	2006	2007
Nombre d'autorisations délivrées	5. 798 (+ 16,5 %)	6.216 (+7 %)	7.085 (+14 %)	9.283 (+30 %)	9.762 (+5,2 %)
Dont autorisations nouvelles	4.657	4.932 (+6 %)	5.882 (+20 %)	6.987 (+17 %)	6.273
Dont autorisations pour des modifications de systèmes existants	1.141	1.284	1.203	2.296	3.489

Source : Ministère de l'intérieur

Cette croissance de la vidéosurveillance dans les espaces publics n'est toutefois pas homogène.

Ces dernières années, les systèmes visionnant la voie publique croissent en effet plus vite.

En 2006, sur 9.283 autorisations délivrées, 8.763 concernaient des systèmes installés dans des lieux ou établissements ouverts au public contre 520 pour des systèmes visionnant la voie publique.

En 2007, sur 9.772 autorisations, 8.395 concernaient des systèmes installés dans des lieux ou établissements ouverts au public contre 1.336 pour des systèmes visionnant la voie publique, dont 756 pour l'installation de nouveaux systèmes. Cette année-là, 14 % des autorisations ont porté sur des systèmes visionnant la voie publique alors que seulement 6 % du stock de caméras déjà installées le sont sur la voie publique.

Les collectivités territoriales, et les communes en particulier, sont les premiers responsables de cette tendance. Selon le ministère de l'intérieur, le nombre de communes ayant recours à la vidéosurveillance, toutes finalités confondues, pour filmer des espaces publics est évalué à 1.522 à la fin 2007 contre 1.142 en 2006 et 812 en 2005.

M. Guy Parayre a indiqué qu'en zone gendarmerie, 325 communes en étaient dotées pour un total de 2.675 caméras.

Enfin, on relèvera que la généralisation des systèmes numériques et la réduction du coût de la conservation des images font que la quasi-totalité des systèmes autorisés permettent une conservation des images d'une durée comprise entre trois et trente jours. Seuls 3 % des systèmes visionnant la voie publique et 5 % des systèmes installés dans lieux et établissements offrent une durée de conservation des images inférieure à 72 heures.

Vos rapporteurs attirent l'attention sur le fait que ces chiffres ne rendent compte que de la vidéosurveillance dans les espaces publics. Ils n'incluent pas les caméras qui n'ont pas à être autorisés, car se trouvant dans des lieux non ouverts au public (domicile, locaux professionnels…). M. Philippe Melchior les a estimées à environ un million.

3. Un marché économique important avec de nouveaux acteurs

Si l'on se réfère à *l'Atlas 2008 de la sécurité, panorama économique du marché de la sécurité*, la vidéosurveillance en France aurait représenté 4,1 % du marché de la sécurité en 2006. Toutefois, il s'agirait de l'un des secteurs les plus dynamiques du marché sur la période récente. Environ 200 entreprises se partageraient un chiffre d'affaires de 750 millions d'euros en progression annuelle de plus de 10 %.

Dans son rapport sur la vidéoprotection[1], l'Institut national des hautes études de sécurité estime qu' « *il s'agit d'un secteur relativement instable marqué par un important éclatement en une multitude de petites entreprises mais connaissant un processus de concentration et de hausse de la pénétration étrangère* ». Il ajoute que « *l'impact de la manne de la commande publique sur ce secteur est à ce jour difficilement mesurable, néanmoins en choisissant comme interlocuteurs privilégiés la dizaine de grandes entreprises dominant actuellement le marché, l'Etat renforce leurs positions internes et en fait des acteurs-clés dans la conception des normes* », ce qui ne serait pas sans conséquence sur le renchérissement des coûts, ces entreprises investissant beaucoup en recherche et développement et proposant des solutions plus complexes là où de petits opérateurs proposent des solutions plus opérationnelles et moins chères.

En outre, vos co-rapporteurs soulignent qu'à côté de ces entreprises spécialisées, les opérateurs de télécommunication classiques comme Orange commencent à entrer sur ce marché, profitant de la convergence des contenus sur le réseau IP (voir I. B. 1) ci-dessus).

Associés aux entreprises spécialisées, ils prennent en charge les coûts d'investissement et de mise à niveau, en contrepartie d'un abonnement par mois et par caméra.

---

[1] *« La vidéoprotection : conditions d'efficacité et critères d'évaluation » mai 2008. pages 6 et 7.*

4. Des finalités nouvelles

La loi du 21 janvier 1995 énumère limitativement les finalités pouvant justifier l'installation de caméras de vidéosurveillance.

Ainsi, sur la voie publique, les autorités publiques compétentes peuvent demander l'autorisation d'installer un système de vidéosurveillance aux fins d'assurer :

- la protection des bâtiments et installations publics et de leurs abords ;

- la sauvegarde des installations utiles à la défense nationale ;

- la régulation du trafic routier ;

- 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 ou de vol ;

- la prévention d'actes de terrorisme.

Les autres personnes morales peuvent également installer des caméras sur la voie publique pour la protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme.

Dans les lieux et établissements ouverts au public, l'installation est possible pour assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol ou sont susceptibles d'être exposés à des actes de terrorisme.

Toutefois, comme le relève la CNIL, on constate une diversification des usages et des finalités de la vidéosurveillance, en dehors du cadre légal.

M. Alain Bauer, président de la commission nationale de la vidéosurveillance, a ainsi souligné la non prise en compte par la législation de certains usages comme la sécurité des clients -hors délinquance- ou l'exploitation d'un service. Il a rappelé que la RATP avait installé les premières caméras sur les quais pour permettre au conducteur de s'assurer qu'aucun passager n'était bloqué entre les portes des wagons. La gestion des files d'attente dans les parcs d'attraction est un autre exemple d'utilisation en dehors des finalités prévues par la loi.

Parmi les autres finalités, la CNIL cite :

- l'utilisation de la vidéosurveillance embarquée dans les véhicules pour la formation des conducteurs de bus ou comme preuve en cas d'accident entre deux véhicules ;

- l'installation de « webcams » par des municipalités sur des sites touristiques ;

- le « vidéoscanning » dans les grandes surfaces qui associe les images des passages en caisse (visionnage des actions de la caissière) et les journaux de caisse. Une telle application constitue une interconnexion de la vidéosurveillance avec le traitement automatisé du logiciel de caisse et est donc susceptible de relever de la compétence de la CNIL ;

- l'enregistrement visuel d'enchères publiques à des fins de preuve de l'adjudication.

M. Philippe Melchior a indiqué à vos rapporteurs que l'exemple du système de vidéosurveillance de voie publique à Strasbourg montrait que seulement un tiers des alertes était destiné à la police municipale ou à la police nationale, les deux tiers intéressant d'autres services (voirie, propreté, pompiers, SAMU…). Les collectivités territoriales ont une interprétation large des finalités de la vidéosurveillance.

M. Sébastien Roché, chercheur au CNRS, estime ainsi qu'« *en une dizaine d'années, la vidéosurveillance est devenue « bonne à tout faire » en matière de gestion de l'espace urbain* »[1].

A cette diversification des usages publics répond une diversification des usages dans les espaces non ouverts au public, donc hors champ de la LOPS du 21 janvier 1995.

5. Des projets de plus en plus intégrés et globaux : l'exemple de la communauté d'agglomération de la vallée de Montmorency

L'essor de la vidéosurveillance s'accompagne d'une professionnalisation de son déploiement. A un certain amateurisme ou improvisation se substitue de plus en plus une conception très en amont associant de multiples acteurs.

A cet égard, vos co-rapporteurs se sont intéressés au système de vidéosurveillance mis en place par la communauté d'agglomération de la vallée de Montmorency (CAVAM) dans le Val d'Oise (95), qui fut le premier exemple de système intercommunal de vidéosurveillance (huit communes représentant 105.000 habitants).

Selon M. Luc Strehaiano, représentant de l'Association des maires de France et président de la CAVAM, quatre ans de réflexion dans le cadre du conseil intercommunal de sécurité et de prévention de la délinquance ont précédé la mise en œuvre du projet qui a duré un an. L'accord entre les communes est intervenu le 24 mai 2006.

---

[1] *In « Les usages techniques et politiques de la vidéosurveillance : une comparaison entre Lyon, Saint-Etienne et Grenoble », rapport de recherche réalisé pour le compte de l'INHES, décembre 2007.*

Ce projet a été mené en partenariat étroit avec la police nationale (deux commissariats). A titre d'illustration, dans chacun des commissariats, les policiers bénéficient non seulement du renvoi d'image mais peuvent également prendre le contrôle des caméras si nécessaire. A moyen terme, les véhicules de la brigade anti-criminalité devraient également bénéficier d'un renvoi d'image par le système GPRS.

En outre, une vraie réflexion a été menée sur les formations des agents chargés du visionnage en temps réel des images.

Opérationnel depuis février 2007, ce système aurait contribué, pour une part qui reste toujours difficile à déterminer, à faire baisser la délinquance de 10 % en 2007 et de 15 à 20 % en mois glissants sur 2008. Sur les six premiers mois de 2008, la vidéosurveillance aurait permis 224 interpellations et 400 interventions.

D. LA PRISE DE CONSCIENCE D'UNE NÉCESSAIRE COORDINATION

1. Un avertissement : l'exemple anglais

Toujours cité comme étant le pays le plus en pointe en matière de vidéosurveillance, en raison principalement de l'étendue de son réseau et du nombre de caméras installées, le Royaume-Uni est un laboratoire privilégié.

Les évaluations les plus avancées sur l'efficacité de la vidéosurveillance aux fins de prévenir la délinquance y ont été réalisées.

L'étude de référence fréquemment citée est celle menée pendant trois ans par M. Martin Gill et Mme Angela Spriggs au nom du Home Office Research, Development and Statistics Directorate[1].

Forte du constat que dans de nombreux cas la vidéosurveillance n'a pratiquement aucun effet sur l'évolution de la délinquance, cette étude conclut néanmoins que la question n'est pas tant de savoir si la vidéosurveillance marche ou non mais dans quelles conditions elle peut être efficace : « *le recours à la vidéosurveillance doit reposer sur une stratégie définissant des objectifs et les moyens pour les atteindre. Cette démarche doit prendre en compte les problématiques de la délinquance locale et les mesures de prévention existantes* ».

Le rapport précité de l'INHES résume ainsi les enseignements des différentes études menées sur la vidéosurveillance : « *pour être efficace, la vidéosurveillance doit être appliquée à certains problèmes qu'elle peut contribuer à traiter et doit être insérée dans une organisation qui permette de tirer parti de ses atouts* ».

[1] *« Assessing the impact of CCTV », Home office research study 292, février 2005.*

Plus récemment encore, en mai dernier, une polémique consécutive aux déclarations de M. Mick Neville, responsable de l'exploitation de la vidéosurveillance à des fins judiciaires à la Metropolitan Police de Londres, a souligné les lacunes de la vidéosurveillance à Londres dont le développement quantitatif – 90.000 caméras contrôlées par les autorités locales- est contrebalancé par un manque de cohérence d'ensemble et des moyens insuffisants pour l'exploitation des images.

N'hésitant pas à parler de fiasco, M. Mick Neville, que vos co-rapporteurs ont rencontré, a indiqué que le Royaume-Uni aurait dépensé au fil des années, plusieurs milliards de Livres Sterling pour mettre en place par strates successives et sans plan d'ensemble, un réseau de vidéosurveillance extrêmement dense afin de prévenir les crimes et délits. Or, outre que l'effet préventif s'estomperait dans le temps, il a jugé le bilan dérisoire en matière judiciaire, l'exploitation des images et leur utilisation comme moyen de preuve au procès pénal n'ayant jamais été sérieusement pris en compte.

La vidéosurveillance comme moyen de preuve au procès pénal

En droit pénal français, les deux règles principales d'admissibilité de la preuve sont la garantie d'un procès équitable et la liberté de la preuve (art.427 du code de procédure pénale.

Le principe étant celui de la liberté, la preuve par la vidéosurveillance est donc recevable. En droit civil, la vidéosurveillance a déjà été admise à titre de preuve en matière de droit du travail dans une affaire de licenciement pour faute grave.

Toutefois, l'admissibilité de la preuve est subordonnée à sa licéité, c'est-à-dire à la manière dont elle a été obtenue. Une image recueillie par un système de vidéosurveillance non autorisé ne pourrait être admise comme preuve.

Enfin, il appartient au juge d'apprécier la fiabilité de la preuve. La qualité de l'image est à cet égard déterminante. Mais même une image ne permettant pas d'identifier un individu peut servir de preuve, par exemple pour déterminer précisément l'heure à laquelle une infraction a été commise.

Toutefois, le fait qu'un enregistrement ne puisse être utilisé comme preuve ne lui retire pas tout intérêt. Il reste un moyen d'investigation important pour orienter l'enquête, par exemple pour connaître les circonstances d'une agression ou la tenue vestimentaire d'un suspect. A défaut de constituer une preuve judiciaire, la vidéosurveillance peut contribuer à la recherche de telles preuves.

Selon son étude, en 2006, seulement 5 % des vols dans les bus auraient été élucidés grâce à la vidéosurveillance alors que chacun est équipé de douze caméras. Or, l'effet préventif ou dissuasif de la vidéosurveillance ne dure pas si elle ne permet pas d'interpeller les délinquants.

M. Mick Neville pointe plusieurs erreurs stratégiques :

- la faible qualité des images ;

- l'absence de formation des policiers à l'utilisation de ces images ;

- la concentration des investissements sur la production des images et non sur leur exploitation par la police à des fins d'investigation et par l'autorité judiciaire comme preuve au procès pénal.

Il a expliqué à vos co-rapporteurs que dans les quartiers où ces erreurs avaient été corrigées, le taux d'élucidation des vols avec violence sur la voie publique avait progressé de 15 à 20 %. **Il a ajouté qu'à terme, la vidéosurveillance deviendrait un outil d'investigation plus efficace que les empreintes génétiques et digitales réunies.** D'ores et déjà, selon une étude comparative entre deux quartiers, l'un sans vidéosurveillance et l'autre avec, si 16 % des crimes seraient élucidés grâce aux empreintes génétiques et digitales pour chacun, 20 % le seraient grâce à la vidéosurveillance pour le second.

2. Le nouvel engagement de l'État en faveur de la vidéoprotection

Il y a encore trois ans environ, l'Etat se tenait en retrait vis-à-vis de la vidéosurveillance[1].

En effet, l'Etat s'est longtemps contenté de fixer le cadre juridique, laissant aux collectivités territoriales, aux transporteurs et aux personnes privées le soin de déterminer leur propre besoin en matière de vidéosurveillance. Aucun dispositif financier, juridique ou politique ne les y incitait. Les renvois d'image vers les commissariats étaient rares et souvent financés par la collectivité elle-même, les services de police ne percevant pas toujours très bien l'intérêt de ces dispositifs. La seule exception concerne la préfecture de police de Paris qui, en raison de ses compétences particulières en matière de police, dispose d'un système de vidéosurveillance de la voie publique. Toutefois, jusqu'à récemment, ce système était assez rudimentaire et dédié à la régulation du trafic routier (voir ci-après).

On évoquera seulement le décret n° 97-46 du 15 janvier 1997 relatif aux obligations de surveillance ou de gardiennage incombant à certains propriétaires, exploitants ou affectataires de locaux professionnels ou commerciaux qui dispose que l'obligation de surveillance de certains de ces locaux[2] **peut être assurée par un système de vidéosurveillance** (articles 3 et 4). Le décret n° 97-47 du 15 janvier 1997 prévoit des dispositions similaires pour la surveillance des garages ou des parcs de stationnement.

Comme le résume le rapport de l'INHES précité, « *l'Etat, à travers la police et la gendarmerie nationales, se positionne ainsi pour la vidéosurveillance de l'espace public comme exploitant secondaire d'images constituées en dehors de lui* ».

Toutefois, cette attitude a changé depuis l'adoption de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

---

[1] *A l'exception de la vidéosurveillance des bâtiments et installations de l'Etat.*
[2] *Les bijouteries et les banques notamment.*

Ce texte marque la première étape de l'implication nouvelle de l'Etat en matière de vidéosurveillance **dans les espaces publics**.

L'article 1er de la loi du 23 janvier 2006 impose désormais que les systèmes de vidéosurveillance soient conformes à des normes techniques nationales minimales. De l'avis général, les critères retenus par l'arrêté du 26 septembre 2006, complété par l'arrêté du 3 août 2007, sont exigeants. Cette normalisation doit améliorer la qualité des systèmes et faciliter leur **interopérabilité**. La mise à niveau des systèmes existants oblige d'ailleurs les opérateurs à des investissements importants.

Cet article 1er a également prévu la possibilité d'un accès direct et permanent des services de police et de gendarmerie aux images des systèmes de vidéosurveillance exploités par des tiers. L'Etat se dote ainsi des moyens d'être destinataire d'images exploitables par ses services.

En outre, l'article 2 de la loi du 23 janvier 2006 a donné au préfet le pouvoir de prescrire la mise en œuvre de systèmes de vidéosurveillance aux fins de prévention d'actes de terrorisme.

Cette première étape fut complétée par la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance[1].

Elle prévoit notamment que lorsqu'un établissement public de coopération intercommunale exerce la compétence relative aux dispositifs locaux de prévention de la délinquance, il peut décider, sous réserve de l'accord de la commune d'implantation, d'acquérir, installer et entretenir des dispositifs de vidéosurveillance. Il peut mettre à disposition de la ou des communes intéressées du personnel pour visionner les images. Cette disposition doit encourager la mise en place de systèmes de vidéosurveillance intercommunaux correspondant à des bassins de délinquance. Elle doit également limiter les effets de report de la délinquance sur les communes voisines. Enfin, elle permet de baisser les coûts en les mutualisant. L'expérience de la communauté d'agglomération de la vallée de Montmorency est exemplaire à cet égard[2].

Par ailleurs, la loi du 5 mars 2007 a créé un Fonds interministériel pour la prévention de la délinquance (FIPD). Ce fonds finance en particulier le raccordement des systèmes de vidéosurveillance aux services de police et de gendarmerie.

Ces ajustements législatifs, qui n'ont toutefois pas modifié le cadre légal général de la vidéosurveillance dans les espaces publics, ont été suivis d'un engagement financier et politique de l'Etat en faveur de cette technologie.

---

[1] On citera également la loi n° 2006-7848 du 5 juillet 2006 relative à la prévention des violences lors des manifestations sportives qui impose, lorsqu'un système de vidéosurveillance est installé dans une enceinte où une manifestation sportive se déroule, de s'assurer, préalablement au déroulement de ladite manifestation, du bon fonctionnement du système de vidéosurveillance.

[2] On relèvera que cette expérience a été lancée avant la loi du 5 mars 2007.

A l'été 2007, le gouvernement sous l'impulsion de Mme Michèle Alliot-Marie a lancé un plan national de développement de la vidéoprotection, l'effort devant porter principalement sur la voie publique et les transports. L'objectif affiché est de tripler en deux ans le nombre de caméras sur la voie publique : 60.000 contre 20.000.

Ce plan s'organise autour de trois axes :

- aider les communes à financer de nouveaux systèmes ;

- raccorder les centres de supervision urbains gérés par les communes aux services de police et de gendarmerie ;

- développer les moyens propres de l'Etat, notamment à Paris avec le plan « 1.000 caméras ».

Un premier bilan peut déjà être fait.

A la fin du premier semestre 2008, le ministère de l'intérieur constatait une hausse des équipements et des demandes d'équipement. En 2007, l'Etat a ainsi contribué au financement de 315 projets, pour un montant total de subvention de 13,4 millions d'euros. 10.000 caméras ont été soumises aux autorisations des préfets en 2007, contre 4.000 en 2006[1].

Toutefois, même si aucune donnée statistique fiable n'est encore disponible, il est probable qu'en 2008 la hausse sera moins importante, les communes ayant procédé aux principaux investissements en 2007 avant les élections municipales.

S'agissant des raccordements entre les centres de supervision et les services de police et de gendarmerie, alors que seulement 61 centres étaient raccordés au 1er juillet 2007, 43 centres supplémentaires l'étaient en juin 2008. 40 raccordements supplémentaires sont attendus pour la fin 2008 et 98 en 2009. Ces investissements sont pris en charge par le FIPD.

S'agissant des moyens propres de l'Etat, outre les caméras embarquées déjà évoquées et les dispositifs mobiles dont la gendarmerie devrait disposer cette année pour réduire le format de certaines gardes statiques, le plan « 1.000 caméras » à Paris est entré dans sa phase de déploiement. En réalité, 1.200 caméras seront installées en surface[2]. L'opération sera pour l'essentiel financée par un partenariat public-privé[3].

---

[1] En zone gendarmerie, près de 200 communes auraient des projets d'équipements, 21 développant des systèmes existants. Sur les 325 communes déjà équipées, seules 11 disposeraient d'un report d'image vers la gendarmerie.

[2] La préfecture de police a déjà accès aux caméras de la RATP et de la SNCF, soit plus de 9.000 caméras.

[3] La ville de Paris participe également au projet, principalement en prenant en charge les travaux de terrassement.

3. Une volonté de pilotage et de cohérence : le comité de pilotage stratégique et la commission nationale de la vidéosurveillance

Cette hausse des moyens consacrés à la vidéosurveillance s'accompagne d'un effort de pilotage inédit.

En premier lieu, à l'initiative du ministre de l'intérieur, **une commission nationale de la vidéosurveillance** a été créée par le décret n° 2007-916 du 15 mai 2007. Installée le 9 novembre 2007, cette commission administrative non prévue par la loi est un organisme consultatif chargé de donner son avis au ministre de l'intérieur sur les évolutions techniques et les principes d'emploi des systèmes de vidéosurveillance. Présidée par M. Alain Bauer, elle se compose de vingt membres désignés pour cinq ans et répartis comme suit :

- sept représentants du ministère de l'intérieur ;

- un représentant du ministère de l'équipement ;

- un représentant du ministère de l'industrie ;

- deux députés et deux sénateurs[1] ;

- le directeur de l'INHES ;

- un représentant de l'Association des maires de France ;

- un représentant de l'Association des maires des grandes villes de France ;

- un représentant des transporteurs publics ;

-un représentant du Conseil national des barreaux ;

- un représentant de l'union des sociétés de protection ;

- un représentant de l'assemblée générale des chambres de commerce et d'industrie.

La composition appelle deux remarques de vos rapporteurs : la surreprésentation de l'Etat (9 membres sur 20 en ne comptabilisant que les représentants des ministères) et la quasi-absence de personnalités qualifiées ou professionnellement sensibles au respect des libertés et de la vie privée.

A côté de cette commission, le ministre de l'intérieur a souhaité se doter d'un Comité de pilotage stratégique, présidé par M. Philippe Melchior.

Composé d'experts, ce comité est chargé de concevoir et d'impulser de nouvelles propositions auprès du ministre de l'intérieur.

Enfin, le Comité interministériel de prévention de la délinquance reste également compétent, notamment pour assurer la cohérence d'ensemble de la politique de prévention de la délinquance dont la vidéosurveillance est un des

[1] *Pour le Sénat, seul notre collègue Christian Cambon a été désigné à ce jour.*

éléments. Le comité interministériel est également attributaire des crédits du Fonds interministériel de prévention de la délinquance. A ce titre, il assure une partie importante de l'ingénierie administrative et financière du plan de développement de la vidéosurveillance.

Ce triple attelage peut se résumer de la façon suivante :

- conception et proposition par le Comité de Pilotage Stratégique ;

- mise en œuvre par le Comité interministériel de prévention de la délinquance ;

- avis et contrôle par la Commission nationale de la vidéosurveillance.

Les raisons de cette implication de l'Etat sont diverses.

En premier lieu, l'exemple anglais montre les erreurs à ne pas reproduire.

En deuxième lieu, la coproduction de sécurité entre les communes et l'Etat semble avoir atteint un nouvel équilibre, de vrais partenariats se nouant. Les maires tentés par la mise en œuvre d'une politique de sécurité concurrente de celle de l'Etat sont de plus en plus rares. Comme l'a déclaré M. Luc Strehaiano, le choix de la communauté d'agglomération de la vallée de Montmorency a été d'offrir à la police nationale un outil de vidéosurveillance performant et adapté à ses besoins, plutôt que de multiplier par deux les effectifs de la police municipale.

En troisième lieu, l'implication de l'Etat témoigne de la prise de conscience que la vidéosurveillance est peu efficace si elle n'est pas organisée pour permettre la répression des infractions. L'effet préventif est en effet très marginal sans répression. Or, la répression relève quasi-exclusivement de la compétence de l'Etat.

Enfin, comme l'a confié M. Frédéric Péchenard, directeur général de la police nationale, le risque est que la multiplication des caméras sans plan d'ensemble et sans que les services de police et de gendarmerie ne soient en capacité de les exploiter utilement n'aboutisse à une mise en cause de la responsabilité de l'Etat par l'opinion publique. Il a expliqué que ce problème se posait déjà avec l'ADN lorsque des faits divers ont montré que si des prélèvements ou des traces avaient été traités en temps utile, des crimes auraient pu être évités. La résorption de ces goulets d'étranglement est un souci constant pour éviter les reproches du type « *vous aviez l'image et vous n'avez rien fait* ».

II. UN RÉGIME JURIDIQUE DÉSORMAIS DÉPASSÉ

A. UNE RÉGLEMENTATION QUI A TRÈS PEU ÉVOLUÉ DEPUIS 1995

1. Les débats préparatoires à la loi du 21 janvier 1995

Face au développement de la vidéosurveillance au début des années 90, une réponse du législateur s'imposait pour encadrer cette technique en raison des risques pour les libertés et la protection de la vie privée.

En l'absence de législation spécifique, plusieurs règles de droit étaient susceptibles de s'appliquer.

● En premier lieu, la législation relative à la protection de la vie privée, résultant de la loi du 17 juillet 1970 sur le droit à l'image (article 9 du code civil et article 226-1 du code pénal).

L'article 226-1 du code pénal disposait et continue à disposer qu' « *est puni d'un an d'emprisonnement et de 45.000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui : [...] 2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans* ***un lieu privé****.* »

Dans les lieux privés ouverts au public (définis par la jurisprudence comme les « *lieux accessibles à tous sans autorisation de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions, heures ou causes déterminées* »), le consentement est présumé si l'intéressé est clairement informé lorsqu'il pénètre dans les lieux qu'il va être filmé.

● En deuxième lieu, la jurisprudence relative au pouvoir de police qui fonde l'intervention de l'autorité administrative pour la préservation de la sécurité et de l'ordre publics **sur la voie publique et dans les lieux publics**.

Ce pouvoir de police doit s'exercer dans le respect du principe de proportionnalité. C'est à ce titre d'ailleurs que le tribunal administratif de Marseille avait annulé le 21 juin 1990 la décision de la ville d'Avignon d'installer un système de vidéosurveillance sur la voie publique.

● En troisième lieu, le droit du travail.

La vidéosurveillance ne doit pas constituer une restriction disproportionnée au but recherché et non justifiée par la nature de la tâche à accomplir. Dans tous les cas, une obligation d'information des salariés demeure. La Cour de cassation a jugé que si un employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu, constitue un mode de preuve illicite (Soc. 20 novembre 1991).

● En quatrième lieu, la législation relative aux casinos ou aux activités privées de surveillance, de gardiennage et de transports de fonds.

En effet, ces sociétés exploitent de nombreux systèmes de vidéosurveillance dans les lieux ouverts ou non ouverts au public, à l'exception de la voie publique. Elles sont soumises à des règles particulières de moralité et de qualification.

● Enfin, la législation relative à l'informatique et aux libertés (loi du 6 janvier 1978).

Toutefois, des divergences d'appréciation existaient sur la portée de cette dernière législation en matière de vidéosurveillance.

Saisie à plusieurs reprises, la CNIL fut conduite à élaborer une doctrine en l'absence de textes spécifiques à la vidéosurveillance. Elle distinguait trois cas :

- 1er cas : la vidéosurveillance faisait appel à des procédés numériques. Pour la CNIL, la loi du 6 janvier 1978 s'appliquait alors dans sa totalité ;

- 2ème cas : le système était analogique, mais il enregistrait les images pendant une certaine durée. La CNIL assimilait ces images enregistrées à une collection de photos susceptibles de contenir des visages identifiables par rapprochement avec un autre fichier. En conséquence, la CNIL considérait les enregistrements comme un fichier non automatisé de données nominatives, auquel étaient applicables les dispositions de fond de la loi du 6 janvier 1978 (information, droit d'accès…). En revanche, les responsables de ces fichiers n'étaient soumis à aucune formalité préalable (déclaration ou autorisation)[1] ;

- 3ème cas : le système était analogique et sans enregistrement. La CNIL ne se considérait pas compétente, la loi du 6 janvier 1978 ne s'appliquant pas.

Cette position est reprise dans la délibération de la CNIL du 21 juin 1994[2] qui affirme que « *les images des personnes doivent être regardées comme des informations nominatives permettant, au moins indirectement, par rapprochement avec d'autres critères, l'identification de ces personnes* ».

Toutefois, cette doctrine de la CNIL n'était pas partagée par la jurisprudence. Ainsi, le Tribunal de grande instance de Paris avait estimé, dans un jugement du 22 mars 1989, que « *ne peut être considéré comme traitement d'informations nominatives au sens de la loi du 6 janvier 1978 [...] le fait pour une société ayant réalisé une image colorisée à partir d'une photographie, de conserver sur ordinateur cette image, sans garder la moindre information relative à la personne photographiée* ». Ainsi, le tribunal refusait-il de considérer qu'une image seule puisse constituer une information nominative, ce qui excluait l'image du champ d'application de la loi du 6 janvier 1978.

---

[1] *A cet égard, saisie pour avis du projet de vidéosurveillance de la ville de Levallois-Perret, la CNIL s'était déclarée non compétente.*

[2] *Délibération n° 94-056 du 21 juin 1994 portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et recevant le public.*

De l'ensemble de ce corpus juridique, ressortait le sentiment d'une grande incertitude et d'une inadaptation des règles de droit en vigueur.

Telle est la raison pour laquelle il a semblé nécessaire de définir un cadre légal spécifique pour la vidéosurveillance sur la voie publique et dans les lieux privés ou publics ouverts au public.

Une première tentative de réponse fut la proposition de loi n° 311 (1992-1993) co-signée par notre ancienne collègue Françoise Séligmann et notre regretté collègue Michel Dreyfus-Schmidt.

Elle proposait notamment que l'installation d'un système de vidéosurveillance de la voie et des lieux publics ne puisse intervenir, quels que soient les procédés techniques utilisés, qu'après avis motivé de la CNIL. En cas d'avis défavorable de celle-ci, il n'aurait pu être passé outre qu'en vertu d'une décision du conseil municipal approuvée par décret pris sur avis conforme du Conseil d'Etat.

Si cette proposition de loi fut une contribution importante au débat, notamment sur la compétence de la CNIL, la loi du 21 janvier 1995 qui a fixé le cadre légal de la vidéosurveillance sur la voie publique et dans les lieux ouverts au public a retenu une autre solution.

2. La loi du 21 janvier 1995 et ses mesures d'application

L'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation pour la sécurité est le principal cadre législatif en matière de vidéosurveillance.

Plusieurs grandes orientations ont été arrêtées.

En premier lieu, ces dispositions spécifiques ne concernent que la vidéosurveillance sur la voie publique et dans les lieux ouverts au public. Les lieux non ouverts au public, privés ou publics, continuent de relever des différentes législations évoquées ci-dessus, lesquels ne sont pas propres à la vidéosurveillance. Il appartient dans ce cas au juge judiciaire d'en apprécier la légalité au regard de la protection de la vie privée, du droit à l'image ou du droit du travail.

En deuxième lieu, le législateur a souhaité trancher le débat sur la compétence de la CNIL en l'écartant, sauf dans le cas où les enregistrements sont utilisés pour la constitution d'un fichier nominatif.

Toutefois, si la compétence de la CNIL est écartée, le législateur s'inspire des principes de la loi du 6 janvier 1978 pour bâtir un dispositif législatif conciliant les nécessités de la prévention de l'ordre public et la protection des libertés. Ces principes sont les suivants :

- principes de licéité et de finalité (les finalités sont fixées par une liste limitative) ;

- conservation des enregistrements limitée (30 jours maximum) ;

- droit d'accès des personnes filmées aux enregistrements ;

- protection des enregistrements ;

- information générale du public sur l'existence d'un système de vidéosurveillance ;

- protection de la vie privée avec l'interdiction de filmer des lieux assimilables à des « informations nominatives sensibles » : intérieur des immeubles d'habitation, y compris l'entrée de ces immeubles.

En troisième lieu, cette législation ne fait pas obstacle à l'application des règles de droit en vigueur relatives, d'une part, au consentement –le cas échéant présumé- de la personne dans les lieux privés ouverts au public (article 226-1 du code pénal) et, d'autre part, aux droits des salariés en tous lieux (code du travail).

En quatrième lieu, la loi du 21 janvier 1995 s'applique, que les images soient enregistrées ou simplement transmises à un poste central. Seul le cas où l'image est directement diffusée sur un moniteur visible de tous, sans enregistrement, échappe à la loi du 21 janvier 1995 (ce type de dispositif est fréquent dans les petits commerces).

En cinquième lieu, la procédure retenue est une procédure administrative d'autorisation. Il s'agit d'un **contrôle a priori**.

L'installation des dispositifs de vidéosurveillance est subordonnée à une **autorisation préfectorale** donnée, sauf en matière de défense nationale, **après avis d'une commission départementale** présidée par un magistrat du siège ou un magistrat honoraire. Le préfet n'est pas tenu de le suivre.

Une autorisation peut être retirée en cas de manquement à la loi ou de modification des conditions au vu desquelles elle a été délivrée. A ce titre, le responsable d'un système est tenu de déclarer toute modification présentant un caractère substantiel.

L'instruction des demandes doit s'attacher à vérifier que, d'une part, les conditions précitées sont réunies et que, d'autre part, **le principe de proportionnalité** est respecté et justifie l'atteinte à la vie privée. Cela implique « *de proportionner l'usage de tels équipements aux risques réellement encourus, compte tenu des circonstances de temps et de lieu, et de choisir en conséquence le nombre, l'emplacement, l'orientation, les caractéristiques des caméras, ainsi que la capacité et la durée de stockage des données* »[1].

Le tableau ci-après synthétise les différentes situations dans lesquelles il est possible d'installer un système de vidéosurveillance sur la voie publique et dans les lieux ouverts au public. Les conditions sont limitatives. Les situations n'entrant pas dans ce cadre sont illicites.

---

[1] *Circulaire du 22 octobre 1996 relative à la réglementation en matière de vidéosurveillance. Elle commente également le décret n° 96-926 du 17 octobre 1996 portant application de l'article 10 de la loi n° 95-73 du 21 janvier 1995. Publiée au Journal officiel du 7 décembre 1996, page 17835.*

La législation en matière de vidéosurveillance des espaces publics

Régime applicable / Finalités de la vidéosurveillance	Lieux susceptibles d'être filmés par les autorités publiques compétentes		Lieux susceptibles d'être filmés par les autres personnes morales		Rôle de la commission départementale		Création par la loi de 2006 d'une procédure d'urgence	Création par la loi de 2006 d'une faculté pour le préfet de prescrire l'installation de vidéosurveillance
	Avant la loi de 2006	**Après la loi de 2006**	**Avant la loi de 2006**	**Après la loi de 2006**	**Avant la loi de 2006**	**Après la loi de 2006**		
Protection des bâtiments et installations publics et de leurs abords, sauvegarde des installations utiles à la défense nationale, régulation du trafic routier, constatation des infractions aux règles de la circulation	- voie publique - lieux et établissements ouverts au public	- voie publique - lieux et établissements ouverts au public	Néant	Néant	- avis préalable à l'autorisation préfectorale délivrée pour une durée indéterminée - contrôle des systèmes sur saisine de toute personne intéressée	- avis préalable à l'autorisation préfectorale délivrée pour une durée de 5 ans renouvelable - contrôle des systèmes sur saisine de toute personne intéressée - pouvoir de contrôle a posteriori sur l'ensemble des systèmes de vidéo-surveillance autorisés	Néant	Néant
Prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression ou de vol	- voie publique - lieux et établissements ouverts au public	- voie publique - lieux et établissements ouverts au public	- lieux et établis-sements ouverts au public	- lieux et établis-sements ouverts au public			Néant	Néant
Prévention d'actes de terrorisme	Néant	- voie publique - lieux et établissements ouverts au public	Néant	- voie publique pour la protection des abords immédiats de leurs bâtiments et installations - lieux et établis-sements ouverts au public exposés à des risques terroristes			- pas d'avis préalable de la commission départementale - autorisation provisoire de quatre mois maximum - avis de la commission avant l'expiration de l'autorisation provisoire	- dans les installations vitales au sens du code de la défense - dans les transports collectifs intérieurs et sur les sites d'infrastructures de transport - la procédure d'urgence peut s'appliquer - la prescription peut porter sur des lieux non ouverts au public

Selon la circulaire du 22 octobre 1996[1], il faut entendre par **autorités publiques compétentes** le préfet ou le maire, mais également les responsables d'établissements ou de services publics et certains concessionnaires comme les concessionnaires d'autoroute.

L'autorisation préfectorale définit **la qualité des personnes chargées de l'exploitation du système de vidéosurveillance ou visionnant les images**. S'il n'est pas nécessaire que ces personnes soient nominativement désignées, il importe en revanche que des garanties de procédures soient données sur leur habilitation et leur formation.

Enfin, l'autorisation fixe le délai maximum de conservation des enregistrements qui ne peut excéder un mois, hormis le cas d'une enquête de flagrant délit, d'une enquête préliminaire ou d'une information judiciaire. Précisons que la conservation des images n'est pas de droit et doit être motivée.

3. La décision du Conseil constitutionnel

Dans sa décision n° 94-352 DC du 18 janvier 1995 relative à la loi d'orientation et de programmation relative à la sécurité, le Conseil constitutionnel a validé la quasi-totalité du dispositif, **tout en prenant soin d'énumérer l'ensemble des dispositions** de nature à concilier la prévention d'atteintes à l'ordre public et la recherche des auteurs d'infractions -objectifs de valeur constitutionnelle- et l'exercice des libertés publiques constitutionnellement garanties au nombre desquelles figurent la liberté individuelle et la liberté d'aller et venir ainsi que l'inviolabilité du domicile[2].

Toutefois, il a censuré la disposition prévoyant que l'autorisation sollicitée pour installer un système de vidéosurveillance est réputée acquise à défaut de réponse dans un délai de quatre mois.

Il a en effet considéré que « *compte tenu des risques que peut comporter pour la liberté individuelle l'installation de systèmes de vidéosurveillance, il ne peut subordonner à la diligence de l'autorité administrative l'autorisation d'installer de tels systèmes sans priver alors de garanties légales les principes constitutionnels ci-dessus rappelés* ».

De cette décision, il peut être déduit que, s'agissant de la vidéosurveillance sur la voie publique et dans les lieux ouverts au public :

- la remise en cause des différentes garanties prévues par la loi ne pourrait se faire sans la plus grande prudence.

---

[1] La circulaire du 22 octobre 1996 relative à la réglementation en matière de vidéosurveillance commente également le décret n° 96-926 du 17 octobre 1996 portant application de l'article 10 de la loi n° 95-73 du 21 janvier 1995. Publiée au Journal officiel du 7 décembre 1996, page 17835.

[2] Le Conseil constitutionnel précise que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle.

- un système d'autorisation expresse est impératif -un simple système déclaratif serait inconstitutionnel ;

- des finalités autres que la prévention de l'ordre public et la recherche des auteurs d'infraction et qui ne constitueraient pas un objectif à valeur constitutionnel ne sauraient probablement justifier à elles seules la mise en place de système de vidéosurveillance.

Sur ce dernier point, on peut s'interroger sur la légalité de l'interprétation faite de la loi du 21 janvier 1995 par la circulaire du 26 octobre 2006. Cette circulaire précise en effet qu'« *une installation de vidéosurveillance motivée exclusivement par une finalité commerciale, fût-elle dans un lieu ouvert au public comme une grande surface, ne rentre pas dans le champ d'application de la loi (du 21 janvier 1995). L'état du droit antérieur en ces cas n'est en rien modifié et la référence au contrat d'adhésion, par une information convenable du public concerné, reste valable* ».

Or, la décision du Conseil constitutionnel est restrictive et n'admet la vidéosurveillance dans les espaces publics que pour les finalités précitées qui relèvent toutes de l'intérêt général. Une simple finalité commerciale est donc certainement illégale.

4. Les résultats en demi-teinte des adaptations de la loi du 23 janvier 2006 relative au terrorisme

La loi du 23 janvier 2006 relative à la lutte contre le terrorisme a apporté plusieurs aménagements à l'article 10 de la loi du 21 janvier 1995. Elle tirait en particulier les conséquences de l'expérience des attentats de Londres qui avaient montré l'utilité de la vidéosurveillance lors de l'enquête.

Plusieurs aménagements ont déjà été présentés (normes techniques minimales, possibilité pour les services de police et de gendarmerie d'accéder en permanence aux images). D'autres modifications méritent également d'être présentées.

● Une nouvelle finalité a été ajoutée : la prévention des actes de terrorisme. Pour cette seule finalité, des personnes morales de droit privé peuvent être autorisées à filmer la voie publique si les lieux sont susceptibles d'être exposés à des actes de terrorisme.

Un premier bilan montre que cette finalité n'a pas fait l'objet d'une utilisation abusive. Outre des grands ports, on notera qu'à Paris, onze systèmes de vidéosurveillance ont été autorisés à ce titre.

● La loi du 23 janvier 2006 a inséré un nouvel article 10-1 dans la loi du 21 janvier 1995 qui permet au préfet d'imposer l'installation d'un système de vidéosurveillance dans certains lieux exposés à des actes de terrorisme.

Toutefois, il semble qu'il n'y ait eu à ce jour très peu de cas d'utilisation de cette procédure, les préfets privilégiant la négociation. Selon le rapport de la commission des lois de l'Assemblée nationale sur l'application de la loi du 23 janvier 2006[1], les négociations achopperaient fréquemment sur la question du financement. Or cette question n'a pas lieu d'être. La loi permet au préfet de prescrire l'installation de la vidéosurveillance sans qu'aucune compensation financière ne soit nécessaire. Le Conseil constitutionnel a validé ces dispositions. En réalité, l'Etat semble avoir fait le choix de ne pas imposer ce que la loi lui permet pourtant de faire.

On notera que le rapport du ministère de l'intérieur à la CNIL pour 2007 sur le bilan de la vidéosurveillance évalue à 6 le nombre de systèmes prescrits par l'autorité préfectorale, notamment dans les Hauts-de-Seine (l'écluse fluviale de Suresnes ainsi que les dépôts pétroliers de Nanterre et Gennevilliers).

● Une procédure d'urgence a été mise en place. Elle permet, en cas d'urgence et d'exposition particulière à un risque terroriste, d'installer un système de vidéosurveillance sans l'avis préalable de la commission départementale. Une autorisation provisoire est délivrée par le préfet pour une durée maximale de quatre mois pendant laquelle la commission départementale rend son avis. Le préfet se prononce alors sur le maintien du système.

Cette disposition n'aurait pas été utilisée jusqu'à présent.

● Les autorisations sont désormais délivrées pour cinq ans et non plus pour une durée illimitée. Les autorisations délivrées antérieurement à la loi arriveront à échéance le 23 janvier 2011. Cette disposition permettra un réexamen régulier de l'utilité des systèmes.

● Enfin, les commissions départementales de vidéosurveillance se sont vues attribuer un pouvoir autonome de contrôle. Elles peuvent s'autosaisir (voir le II.C.2. ci-dessous).

B. DES CONFLITS DE COMPÉTENCE NON TRANCHÉS

1. Le débat sur la compétence de la CNIL

Comme il a été vu ci-dessus, avant la loi du 21 janvier 1995, la doctrine était déjà divisée sur la compétence de la CNIL en matière de vidéosurveillance.

Pour cette raison, en 1995, le législateur a souhaité trancher ce débat. La compétence de la CNIL a été écartée, le texte adopté disposant sans ambiguïtés que « *les enregistrements visuels de vidéosurveillance ne sont considérés comme des informations nominatives, au sens de la loi du 6 janvier 1978 […], que s'ils sont utilisés pour la constitution d'un fichier nominatif* ».

[1] http://www.assemblee-nationale.fr/13/pdf/rap-info/i0683.pdf.

Les raisons de ce choix étaient diverses :

- la charge de travail déjà excessive de la CNIL ;

- l'éloignement de la CNIL, l'examen de chaque demande d'installation exigeant de bien connaître les situations locales ;

- le rejet de l'argument selon lequel tout système numérique serait constitutif d'un traitement automatisé ;

- une jurisprudence qui refuse d'assimiler les enregistrements analogiques à une succession de photos constituant chacune une information nominative en tant que telle.

Cette rédaction avait également pour effet d'écarter la compétence de la CNIL pour **tous les systèmes de vidéosurveillance**, y compris ceux ne relevant pas de la loi du 21 janvier 1995, c'est-à-dire ceux installés dans les lieux non ouverts au public.

Toutefois, la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pour la protection des données a sensiblement modifié cet équilibre.

Si la loi continue d'écarter la compétence de la CNIL pour les systèmes de vidéosurveillance relevant de la loi du 21 janvier 1995, sauf si les enregistrements sont utilisés dans un traitement automatisé –dans ce cas, la CNIL a une compétence exclusive-, en revanche :

- elle ne dispose plus explicitement que les enregistrements ne sont pas des informations nominatives, donc insusceptibles d'entrer dans le champ de la loi du 6 janvier 1978 ;

- elle n'exclut plus la compétence de la CNIL et l'application de la loi du 6 janvier 1978 pour les enregistrements de vidéosurveillance ne relevant pas de la loi du 21 janvier 1995.

Il en résulte que la CNIL est compétente pour les systèmes de vidéosurveillance dans les lieux non ouverts au public au sens de la jurisprudence. Tel est notamment le cas des entrepôts ou des locaux réservés à l'usage des personnels (dans ces lieux, le code du travail et la législation sur le droit à l'image s'appliquent également).

On ajoutera que la loi du 21 janvier 1995 modifiée par la loi du 6 août 2004 prévoit désormais que le Gouvernement transmet chaque année à la CNIL un rapport faisant état de l'activité des commissions départementales chargées d'émettre un avis et de contrôler les systèmes de vidéosurveillance et, de manière plus générale, des conditions d'application de cette législation.

Enfin, la loi du 6 août 2004 a considérablement élargi le champ d'application de la loi du 6 janvier 1978.

L'article 2 de la loi du 6 janvier 1978 dispose désormais que :

« *La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers […].*

« *Constitue une donnée à caractère personnel*[1] *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*

« *Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.*

« *Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.* »

Tant la définition des données à caractère personnel que celle des traitements automatisés offrent des arguments en faveur d'une reconnaissance de la compétence de la CNIL en matière de vidéosurveillance dès lors que celle-ci donne lieu à enregistrement et utilise la technologie numérique.

Enfin, les perspectives de développement de la biométrie, en particulier de la reconnaissance faciale, relèvent incontestablement de la CNIL. Les traitements ayant recours à des techniques biométriques sont en effet soumis sans exception à une procédure d'autorisation préalable par la CNIL, en vertu notamment des articles 25-8° et 27 de loi « informatique et libertés ».

Ces modifications législatives ainsi que la généralisation de la technologie numérique ont relancé les débats sur la compétence de la CNIL en matière de vidéosurveillance des espaces publics.

---

[1] *La loi du 6 août 2004 a substitué la notion de « données à caractère personnel » à celle « d'informations nominatives ». Les informations nominatives étaient définies comme celles permettant « sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale ».*

2. Des distinctions subtiles selon le lieu et la technologie utilisée

Dans une note publique au ministre de l'intérieur, la CNIL a récemment exposé son analyse relative aux autorités compétentes en matière de vidéosurveillance.

a) Les systèmes numériques : qui est compétent ?

Quelques points ne semblent pas prêter à discussion.

● La CNIL est compétente lorsqu'un dispositif de vidéosurveillance est installé dans **un lieu non accessible au public** (entrepôts, réserves, bureaux fermés au public) et que les images sont enregistrées ou conservées sur un support informatisé de type disque dur ou enregistreur numérique, ce qui est le cas de la quasi-totalité des systèmes actuellement dans le commerce.

On précisera que conformément à l'article 2 de loi du 6 janvier 1978, les traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles ne sont pas soumis à cette législation. Il en résulte que l'installation par un particulier d'un système de vidéosurveillance filmant l'intérieur de son domicile privé ou l'intérieur des limites de sa propriété n'est pas soumise à déclaration préalable auprès de la CNIL.

Elle est également compétente dans tous les cas et quel que soit le lieu lorsqu'une technique biométrique est couplée à un système de vidéosurveillance.

● L'autorité préfectorale est compétente pour l'ensemble des systèmes analogiques. Ceux-ci sont toutefois en voie de disparition.

De même, les systèmes prévoyant uniquement la visualisation sans enregistrement d'images de la voie publique ou d'un lieu ouvert au public, que ces systèmes soient numériques ou analogiques, relèvent de la compétence du préfet. La CNIL ne considère pas la seule visualisation d'images comme un traitement automatisé au sens de la loi « informatique et libertés ».

En revanche, les systèmes numériques de vidéosurveillance avec enregistrement sur la voie publique ou dans les lieux ouverts au public suscitent une controverse importante.

La CNIL estime qu'un système de vidéosurveillance, **dès lors qu'il est numérique**, entre dans le champ d'application de la loi « informatique et libertés ».

Cette analyse se fonde sur la nouvelle définition des « données à caractère personnel » et des « traitements automatisés » issue de la loi du 6 août 2004. Tout système numérique répondrait ainsi à la qualification de « traitement automatisé » et devrait faire l'objet d'une déclaration à la CNIL.

Vos co-rapporteurs ont interrogé les différentes personnes auditionnées sur cette interprétation de la CNIL.

Force est de reconnaître que les avis sont très divergents, le ministère de l'intérieur la rejetant[1].

Plusieurs remarques peuvent toutefois être faites.

Tout d'abord, le législateur a clairement souhaité que la loi du 21 janvier 1995 prévoyant la compétence du préfet s'applique aux systèmes de vidéosurveillance de la voie publique et des lieux ouverts au public, sans considération de la technologie utilisée.

L'exception disposant que les enregistrements visuels de vidéosurveillance utilisés dans des traitements automatisés ou contenus dans des fichiers structurés relèvent de la loi du 6 janvier 1978 est peut-être mal rédigée, mais il est certain que la volonté du législateur n'était pas d'exclure la compétence du préfet dès qu'un système est numérique. Cette exception ne vise que le cas où un système de vidéosurveillance est couplé à un véritable fichier permettant d'identifier, directement ou indirectement, les personnes filmées.

Par ailleurs, tout en reconnaissant la validité des arguments de la CNIL quant à sa compétence, celle-ci ne peut écarter la compétence du préfet. Si la loi « informatique et libertés » est une loi générale, la loi du 21 janvier 1995 modifiée est une loi spéciale et l'emporte donc.

Pour concilier ces différents points de vue, on peut admettre une compétence conjointe. Autrement dit, une personne souhaitant installer un système de vidéosurveillance numérique dans un espace public doit, d'une part, obtenir l'autorisation du préfet et, d'autre part, déclarer ce système à la CNIL.

Sans trancher définitivement le débat, il faut souligner, à la suite de la CNIL au demeurant, « *l'extrême gravité du problème posé, compte tenu du fait que la concurrence des 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.* »

A cet égard, la CNIL est de plus en plus saisie par des citoyens et des responsables de traitement de la question de savoir si les dispositifs de vidéosurveillance doivent également lui être soumis, si elle est exclusivement compétente, ou s'il est nécessaire de saisir les commissions départementales.

---

[1] *La circulaire du 22 octobre 1996 relative à l'application de la loi du 21 janvier 1995 dans sa version initiale écarte clairement la compétence de la CNIL. Elle mériterait néanmoins une mise à jour étant donné qu'elle ne tient pas du tout compte des modifications consécutives à la loi du 6 août 2004.*

b) Le problème des lieux mixtes

La loi du 21 janvier 1995 est relative à la vidéosurveillance sur la voie publique et dans les lieux et établissements ouverts au public.

La définition jurisprudentielle des lieux ouverts au public est relativement claire. Un jugement du Tribunal de grande instance de Paris du 13 octobre 1986 confirmé par la Cour d'appel le définit comme « *un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions* » comme un droit d'entrée.

Un véhicule pourra être considéré comme tel. C'est le cas des bus des lignes de transport public. Par contre, les cars des lignes à longue distance seront considérés comme des lieux non ouverts au public, parce qu'il faut généralement réserver et acquitter le prix du voyage à l'avance. Un établissement scolaire est également considéré comme un lieu non ouvert au public.

Toutefois, cette distinction entre les lieux ouverts et non ouverts au public aboutit dans de nombreux cas à appliquer deux régimes juridiques –loi du 21 janvier 1995 et loi du 6 janvier 1978- à un même système de vidéosurveillance.

En effet, de nombreux bâtiments ou espaces sont des lieux mixtes : une partie des locaux est ouverte au public, une autre ne l'est pas.

Or, le responsable de ce bâtiment prévoira généralement un système de vidéosurveillance à la fois dans une zone ouverte au public et dans une ou plusieurs zones non accessibles au public.

Il en est ainsi pour les grandes surfaces de distribution, au sein desquelles un même système de caméras surveille à la fois une zone ouverte au public (les rayons de la surface de vente), et des zones non accessibles au public (réserves, quais de déchargement) accessibles uniquement aux employés.

Chaque zone obéit alors à des régimes juridiques distincts.

C. DES PROCÉDURES NON OPTIMALES

1. Des décisions peu homogènes

M. Philippe Melchior, président du Comité de pilotage stratégique de la vidéosurveillance, a expliqué que l'application de la loi du 21 janvier 1995 n'était pas homogène. Cela se traduit en particulier par des décisions divergentes lorsque par exemple une chaîne de magasins implantés sur l'ensemble du territoire dans des conditions similaires décide d'équiper chacune de ses succursales avec de la vidéosurveillance.

2. Le fonctionnement disparate des commissions départementales

La commission départementale des systèmes de vidéosurveillance comprend désormais quatre membres :

- le président, magistrat de l'ordre judiciaire comme la loi le prévoit ;

- un maire, désigné par les associations départementales des maires ;

- un représentant désigné par la ou les chambres de commerce et d'industrie territorialement compétentes ;

- une personnalité qualifiée choisie en raison de sa compétence par le préfet.

Initialement, le décret n° 96-926 du 17 octobre 1996 fixait à cinq le nombre de membres de la commission. Il prévoyait la présence d'un magistrat de la juridiction administrative. Toutefois, l'article 60 du décret n° 2006-665 du 7 juin 2006 relatif à la réduction du nombre et à la simplification de la composition de diverses commissions administratives a supprimé la présence d'un magistrat de la juridiction administrative.

Le mandat est de trois ans. Il peut être renouvelé une fois.

La commission départementale remplit deux fonctions.

Elle a tout d'abord un rôle consultatif. Elle rend un avis sur chaque demande d'installation de vidéosurveillance.

Elle assure aussi des fonctions de contrôle.

Jusqu'à la loi du 23 janvier 2006, la commission n'avait pas la possibilité de se saisir elle-même des conditions de fonctionnement d'un système de vidéosurveillance. Elle devait être saisie par « toute personne intéressée » -par exemple les personnes rencontrant une difficulté pour faire valoir leur droit d'accès aux images les concernant.

La loi du 23 janvier 2006 a consacré un pouvoir autonome de contrôle sur les conditions de fonctionnement des systèmes de vidéosurveillance. Elle peut émettre des recommandations et proposer la suspension des dispositifs lorsqu'elle constate qu'il en est fait un usage anormal ou non conforme à leur autorisation.

En outre, l'article 4 du décret n° 2006-929 du 28 juillet 2006 permet à la commission de désigner un de ses membres pour collecter des informations relatives aux conditions de fonctionnement d'un système de vidéosurveillance. Cette disposition est censée augmenter et faciliter les activités de contrôle.

Quel bilan peut-on faire des commissions départementales ?

S'agissant de leur rôle consultatif, le bilan est mitigé.

La périodicité des réunions se situe en moyenne entre trois et quatre mois. Dans les départements très urbanisés, les réunions sont toutefois plus fréquentes. Ce délai pose un problème car le silence de l'administration pendant quatre mois vaut rejet de la demande.

Aussi, le ministère de l'intérieur préparerait-il un décret prévoyant qu'en cas de silence de la commission durant trois mois, l'avis est réputé reçu. Ceci permettrait au préfet de statuer sur une autorisation d'installation, dans le délai de quatre mois qui lui est imposé.

La non-permanence de ces commissions, leur petite taille et leur composition en font des organes mal outillés pour développer une expertise technique pointue et pour vérifier la nécessité de chacun des systèmes. Selon la Ligue des droits de l'homme, les membres des commissions départementales se déplaceraient très rarement sur le terrain pour procéder aux vérifications nécessaires.

Si dans les départements les plus urbanisés, le volume de travail permet aux commissions d'acquérir plus rapidement une expertise, ce n'est pas le cas dans les autres départements. Il en résulte des divergences d'appréciation.

En revanche, au crédit de ces commissions, il faut reconnaître que si l'avis est simplement consultatif, en pratique le préfet le suit presque toujours.

S'agissant de leurs fonctions de contrôle, le bilan est assez maigre.

En 2004, 942 contrôles ont été ainsi opérés dont 17 % ont donné lieu à constatation d'infraction.

En 2006, alors que l'on pouvait s'attendre à une hausse des contrôles du fait de l'attribution d'un pouvoir d'autosaisine, leur nombre était en baisse. 869 contrôles avaient été réalisés, dont 22 % avaient donné lieu à la constatation d'infractions.

En 2007, la baisse s'est poursuivie[1]. Seulement 483 contrôles ont été effectués au lieu de 869 en 2006. Selon le ministère de l'intérieur, le nombre important de contrôles effectués en 2006 s'expliquerait par des campagnes de contrôles entreprises à l'initiative des services de police et de gendarmerie dans plusieurs départements. Cette pratique ne semble pas avoir été renouvelée cette année. En 2006, 22 % des contrôles effectués avaient donné lieu à la constatation d'une infraction.

Seuls 11 % des contrôles mis en œuvre en 2007 ont donné lieu à la constatation d'infractions dont les principales se répartissent comme suit :

- fonctionnement de systèmes sans autorisation (67 %) ;

- insuffisance de l'information du public quant à l'existence des caméras (16 %) ;

---

[1] *La majorité des contrôles effectués en 2007 l'a été à l'initiative des commissions départementales (93,6% contre 6,4% sur l'initiative d'un particulier).*

- visionnage de la voie publique non autorisé (2 %) ;

- conservation des enregistrements au-delà de la durée autorisée (2 %).

En outre, les recommandations et avis n'étant pas publics, ces commissions intimident peu les responsables de système de vidéosurveillance tant qu'ils n'ont pas fait l'objet de contrôle.

Les points faibles des commissions départementales peuvent expliquer le développement de chartes d'éthique ou de codes de bonne conduite dans les villes faisant le choix de la vidéosurveillance.

Ainsi, la ville de Lyon a créé un collège d'éthique par délibération du conseil municipal du 14 avril 2003. Il se compose à part égale d'élus de la majorité et de l'opposition, de personnalités qualifiées représentant le monde du droit, de l'économie et de l'éducation et de représentants d'associations de défense des droits de l'homme.

Il est chargé de veiller, au-delà du respect des obligations législatives et réglementaires, à ce que le système de vidéosurveillance mis en place par la ville ne porte pas atteinte aux libertés publiques et privées fondamentales. Il peut s'autosaisir et recevoir des doléances.

3. De nouvelles utilisations de la vidéosurveillance mal prises en compte par les textes

Comme l'a rappelé M. Philippe Melchior, lors de l'adoption de la loi du 21 janvier 1995, les responsables politiques n'avaient pas encore une idée précise de l'utilisation de la vidéosurveillance. Du fait des circonstances et en particulier de la polémique relative au projet de la ville de Levallois-Perret, **le législateur a retenu pour seule grille de lecture la finalité de protection de la sécurité publique.**

Ainsi, les finalités de la vidéosurveillance dans les espaces publics sont définies de façon réductrice comparée à l'usage qu'en ont les communes aujourd'hui. Compte tenu du coût de ces systèmes, des communes cherchent à amortir l'investissement en diversifiant les applications (voirie, entretien, secours…).

Or, la loi ne prévoit pas ces finalités. La décision du Conseil constitutionnel incline à penser que si elles ne sont pas prévues, elles sont donc a priori interdites.

Toutefois, on imagine mal revenir en arrière tant la vidéosurveillance est devenue dans certaines villes un mode de gestion urbaine.

Une autre difficulté déjà évoquée tient au développement récent des dispositifs mobiles ou provisoires de vidéosurveillance. Le nombre de ces dispositifs devrait être décuplé dans les prochaines années, la police et la gendarmerie souhaitant en acquérir massivement, soit dans les véhicules, soit sur les agents.

Or, la loi du 21 janvier 1995 ne prévoit aucune disposition spécifique[1] alors que ces dispositifs se concilient difficilement avec certains principes comme l'information du public[2], à moins de considérer que ces caméras ne relèvent pas de ce cadre légal. Ces caméras ne seraient pas assimilables à de la vidéosurveillance ; elles ne seraient que le prolongement de l'œil des policiers et gendarmes.

En tout état de cause, une clarification juridique est sans doute nécessaire.

Il en est également ainsi pour les dispositifs de vidéosurveillance fixes mais provisoires. Le Général Guy Parayre, ancien directeur général de la gendarmerie nationale, a ainsi fait part des projets de développement de systèmes de vidéosurveillance provisoires, faciles à déplacer, afin de répondre ponctuellement à des besoins. En effet, des évènements comme des concerts, des ferias, des raves, des courses automobiles ou des sommets de chefs d'Etat pourraient utilement faire l'objet de vidéosurveillance.

Toutefois, la procédure ne s'y prête pas, à moins que la finalité ne soit la prévention d'actes de terrorisme. Dans ce cas, une procédure d'urgence sans avis préalable de la commission départementale peut être activée. Dans tous les autres cas, les délais rendent la mise en œuvre difficile. La loi du 21 janvier 1995 apparaît donc mal taillée.

Or, à bien des égards, un dispositif temporaire est préférable à un système permanent. Il est notamment plus conforme aux principes de finalité et de proportionnalité.

III. LES RECOMMANDATIONS DU GROUPE DE TRAVAIL

A. RÉUNIR SOUS UNE SEULE AUTORITÉ, LA CNIL, LES COMPÉTENCES D'AUTORISATION ET DE CONTRÔLE EN MATIÈRE DE VIDÉOSURVEILLANCE

Comme on l'a vu, les conflits de compétence entre la CNIL et le préfet en matière de vidéosurveillance des espaces publics sont importants. Par ailleurs, le contrôle n'est pas satisfaisant à l'heure actuelle.

Vos co-rapporteurs estiment que la solution la plus simple et la plus cohérente consisterait à attribuer à la CNIL la compétence pour autoriser et contrôler l'installation de systèmes de vidéosurveillance dans les espaces publics.

---

[1] Toutefois, l'article 2 du décret n° 96-926 du 17 octobre 1996 évoque indirectement ce cas de figure en disposant que l'utilisation de « dispositifs mobiles de surveillance de la sécurité routière » s'oppose à la transmission de certains documents lors de la demande d'autorisation, en particulier le plan masse des lieux filmés et le plan d'implantation des caméras.

[2] Toutefois, on peut estimer que l'uniforme de l'agent ou la sérigraphie du véhicule suffit déjà à informer le public qu'il est surveillé.

1. Régler définitivement les conflits de compétence

Plusieurs facteurs militent en ce sens.

En premier lieu, la CNIL est d'ores et déjà confrontée à cette question. Dans son rapport d'activité pour 2007, elle constate depuis cinq ans un fort accroissement des formalités déclaratives relatives à la vidéosurveillance.

Le nombre de déclarations est en augmentation constante depuis 2002, avec des augmentations fortes en 2004 (quatre fois plus qu'en 2003) et 2006 (trois fois plus de dossiers qu'en 2005). L'augmentation se poursuit en 2007 avec 1.317 déclarations enregistrées pour un total de 2.980 déclarations sur la période 2002-2007. Dans la majorité des cas, la déclaration concerne plusieurs caméras.

Ces déclarations portent principalement sur des systèmes de vidéosurveillance des lieux non ouverts au public, la CNIL ayant une compétence certaine pour la vidéosurveillance numérique dans ces lieux. Mais notre collègue Alex Türk, président de la CNIL, a indiqué que ses services étaient quotidiennement confrontés à de très nombreuses demandes du public et de professionnels, tant téléphoniques qu'écrites, quant au régime juridique applicable en matière de vidéosurveillance dans les espaces publics.

En deuxième lieu, il faut rappeler que si la loi du 21 janvier 1995 n'attribue pas la compétence à la CNIL pour autoriser les systèmes de vidéosurveillance dans les espaces publics, en revanche elle s'inspire directement des principes de la loi du 6 janvier 1978 : proportionnalité, finalité, information du public, droit d'accès… Cette filiation faciliterait le transfert de compétences.

En troisième lieu, une autorité unique présenterait incontestablement l'avantage d'une meilleure homogénéité des décisions.

En quatrième lieu, la CNIL serait compétente aussi bien dans les lieux non ouverts au public que dans les espaces publics. Certes, les procédures ne seraient pas fusionnées, la décision du Conseil constitutionnel exigeant que la vidéosurveillance dans les espaces publics soit soumise à une procédure d'autorisation expresse et non à une simple déclaration comme c'est aujourd'hui le cas dans les lieux non ouverts au public. Mais il reviendrait à un même organe de connaître de ces deux types de lieux, ce qui faciliterait la gestion des dossiers compte tenu de l'imbrication de ces espaces.

Pour l'usager, il en résulterait une simplification importante, d'autant que la CNIL jouit d'une forte notoriété. Elle serait son interlocuteur unique.

Enfin, vos co-rapporteurs attirent l'attention sur les évolutions à venir de la vidéosurveillance.

Les systèmes de vidéosurveillance biométriques ou intelligents, c'est-à-dire permettant de programmer a priori les types de comportement à identifier, sont appelés à se développer. Comme l'explique M. Jean-Jacques Froment, professeur de droit public à la faculté de Grenoble,[1] « *ces nouveaux systèmes déplacent nombre d'interrogations sur les libertés, en diminuant certains des risques traditionnels (allègement de la charge de la surveillance tant sur le plan spatial que temporel) et en créant dans le même temps de nouveaux risques (risque de stigmatisation discriminante de certaines catégories de population, émergence de nouvelles finalités, disproportion des moyens employés* ».

D'ores et déjà, les systèmes de vidéosurveillance biométriques sont exclusivement de la compétence de la CNIL. Le régime juridique des « vidéo-intelligentes » sans biométrie n'est pas clairement défini, mais la complexité des questions posées au regard de la protection des libertés individuelles plaide en faveur de la compétence de la CNIL.

Compte tenu de l'essor probable de ces systèmes[2], le maintien du statu quo aurait pour effet de morceler encore un peu plus le régime juridique de la vidéosurveillance. L'unicité de la compétence de la CNIL aurait pour avantage d'anticiper les développements technologiques futurs et d'éviter d'être contraint d'adapter avec retard notre législation.

2. Le choix de la CNIL plutôt que d'une commission ad hoc

Une autre solution consisterait à confier les attributions actuelles des préfets et des commissions départementales à une autorité administrative indépendante spécialisée, dont la commission nationale de la vidéosurveillance serait le précurseur.

Si cette solution présente des avantages communs avec la première évoquée (homogénéité des décisions en particulier), elle présente plusieurs inconvénients.

Tout d'abord, à la suite des travaux de notre collègue Patrice Gélard sur les autorités administratives indépendantes (AAI)[3], votre commission des lois est opposée à en créer de nouvelles, très spécialisées, dans des secteurs connexes à des AAI déjà en place. Or, en l'espèce, force est de reconnaître que la CNIL a toujours conservé la vidéosurveillance dans son champ de vision. Au surplus, l'attribution de cette compétence supplémentaire à la CNIL coûterait certainement moins cher.

---

[1] In « Regard juridique sur la vidéosurveillance urbaine : un droit en trompe l'œil » La semaine juridique. N° 13, 27 mars 2006.

[2] A ce jour, ces cas de figure sont très marginaux. On notera également que Sur 10.819 demandes reçues en 2007, l'autorité préfectorale a estimé dans seulement 14 cas que le système de vidéosurveillance dont elle était saisie permettait un couplage avec un fichier relevant de la compétence exclusive de la CNIL.

[3] Rapport n° 404 (2005-2006) « Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié » au nom de l'Office parlementaire d'évaluation de la législation.

Surtout, il semble important à vos co-rapporteurs au moment où les technologies de l'information et de traçage se développent à une vitesse exponentielle de conserver une vue d'ensemble sur tous ces enjeux.

En effet, prise isolément, chaque technologie de l'information présente des risques au regard des libertés individuelles et du respect de la vie privée, mais ces risques restent généralement tolérables et maîtrisables. En revanche, l'addition de chacune de ces technologies et des données personnelles ainsi emmagasinées –cartes de crédit, géolocalisation, téléphone, vidéosurveillance, documents d'identité biométrique, réseaux sociaux…- peut mettre en cause directement l'intégrité de notre vie privée et de nos libertés individuelles.

M. Alex Türk, président de la CNIL, a notamment alerté vos co-rapporteurs sur la situation dans les aéroports où la multiplication des mécanismes de contrôle[1] aboutit à une mise à nue, au sens propre comme figuré, des voyageurs.

C'est la raison pour laquelle la CNIL est l'autorité la mieux préparée pour assurer cette mission compte tenu de sa taille, de son ancienneté, de sa notoriété et de son indépendance reconnue.

3. Pour un vrai contrôle

Le contrôle s'exerce à deux moments : a priori et a posteriori.

Le contrôle a posteriori appartient aujourd'hui aux commissions départementales de vidéosurveillance. Le préfet en connaît également, en particulier depuis que la loi du 23 janvier 2006 dispose que l'autorisation est délivrée pour une durée de cinq ans. Cela signifie qu'à partir de 2011, les préfets auront à faire le point sur les systèmes déjà autorisés.

Toutefois, les témoignages des différentes personnes entendues montrent que ces mécanismes de contrôle a posteriori fonctionnent mal. Les principaux défauts sont la non permanence des commissions départementales et leur manque d'expertise technique.

L'attribution de cette mission à la CNIL[2] permettrait au contraire de professionnaliser le contrôle. En effet, la technicité de la matière requiert des contrôleurs professionnels qui soient crédibles face aux responsables des systèmes et aux industriels. La CNIL dispose naturellement de cette expérience et de la taille critique.

En outre, la notoriété de la CNIL et sa visibilité inciteraient un plus grand nombre de personnes à signaler des dysfonctionnements, des utilisations abusives, voire des systèmes installés sans autorisation en toute illégalité.

---

[1] *On citera les passeports biométriques, les données PNR, le « body scanning », l'insertion de puces RFID sur les billets, la vidéosurveillance…*

[2] *Du fait des interstices de la législation et de la compétence de la CNIL.*

Toutefois, le premier contrôle intervient au moment de la délivrance de l'autorisation. Il s'agit en particulier de s'assurer du respect des finalités prévues par la loi, de la nécessité du système et de la proportionnalité du dispositif choisi.

La procédure en vigueur pour la vidéosurveillance des espaces publics attribue cette compétence au préfet.

Le choix du préfet n'était pas contestable en 1995, lorsque l'intérêt de la vidéosurveillance n'était pas bien identifié et l'Etat n'était pas un partisan du développement de la vidéosurveillance. Le préfet apparaissait alors comme un tiers neutre chargé d'appliquer une législation restrictive et conçue pour permettre la vidéosurveillance, mais sans la faciliter.

Cet équilibre n'existe plus aujourd'hui. Le cadre légal est resté quasi-identique, mais l'Etat est devenu un promoteur de la vidéosurveillance.

Le plan national de développement de la vidéosurveillance aboutit à une co-production en matière de sécurité, associant les collectivités, des partenaires privés et les services de police et de gendarmerie. Ces derniers grâce au raccordement d'images figurent parmi les principaux bénéficiaires des systèmes de vidéosurveillance.

Dans certains cas, le préfet autorisera des systèmes de vidéosurveillance après avoir participé à leur élaboration dans le cadre des conseils locaux de sécurité et de prévention de la délinquance, voire à leur financement. Le préfet se trouve malgré lui en position de juge et partie.

Toutefois, ces observations ne doivent pas être mal interprétées. Elles n'ont pas pour objet de faire le procès des préfets qui appliquent la loi. Les données disponibles montrent d'ailleurs qu'une proportion significative des demandes d'installation de système de vidéosurveillance fait l'objet d'un refus.

En 2007, 790 refus ont été opposés à des demandes d'autorisation (+ 155 % par rapport au 309 refus enregistrés en 2006) pour 9.762 autorisations délivrées.

Les motifs de refus sont :

- un dossier incomplet (39 %) ;

- un système hors du champ de la loi (32 %) ;

- l'absence de risque particulier d'agression, de vol ou de terrorisme (9 %) ;

- une atteinte disproportionnée aux libertés individuelles (7 %) ;

- une finalité non conforme à la réglementation (3 %) ;

- la visualisation de la voie publique par une autorité non compétente (2 %) ;

- une information insuffisante du public (2 %) ;

- autre (6 %).

Le ministère de l'intérieur observe que l'augmentation, par rapport à 2006, du nombre de dossiers d'autorisation refusés, porte essentiellement sur des dossiers jugés incomplets (39 % des motifs de refus au lieu de 25 % en 2006) ou concernant des systèmes hors du champ de la loi (32 % des motifs de refus au lieu de 20 % en 2006). Inversement, l'absence de risque d'agression, de vol ou d'acte de terrorisme ne représente que 9 % des motifs soit deux fois moins qu'en 2006. De même, les dossiers refusés pour atteinte disproportionnée aux libertés individuelles représentent 7 % des refus en 2007 au lieu de 15 % en 2006.

Ces variations sont délicates interprétées : soit les demandes ont changé de nature, soit les préfectures procèdent à un examen plus formel des dossiers.

4. La CNIL en a-t-elle les moyens ?

La principale objection à la compétence de la CNIL est son manque de moyens, celle-ci ayant déjà des difficultés à faire face à ces missions actuelles.

En outre, l'éloignement de la CNIL à Paris rendrait son action largement théorique et la déconnecterait des conditions réelles d'implantation des caméras.

S'agissant des moyens, on observera tout d'abord que ceux-ci sont en hausse régulière depuis quelques années. En 2008, les crédits votés en loi de finances initiale se sont élevés à 11,33 millions d'euros. Pour 2009, le projet de loi finances prévoit une dotation de près de 13 millions, en hausse de +14 %.

En outre, il est toujours possible de les augmenter pour faire face à ces nouvelles missions. Certes, le contexte budgétaire très contraint ne plaide pas en faveur de cette solution. Mais, il serait certainement possible de réaffecter à la CNIL les montants correspondants au coût des commissions départementales. Leurs membres sont en effet rémunérés sous forme de vacations horaires et les frais de transports et de séjour peuvent être remboursés. Toutefois, vos co-rapporteurs ne disposent pas d'une évaluation du montant total de ces sommes.

S'agissant du risque bureaucratique, il convient tout d'abord de ne pas surestimer le travail de terrain des commissions départementales et des services préfectoraux. L'examen des demandes repose avant tout sur l'étude du dossier et des nombreux documents exigés par le décret du 17 octobre 1996. En outre, le travail des commissions se concentre essentiellement sur la phase d'autorisation administrative, la plus procédurière, et très peu sur le contrôle a posteriori.

Par ailleurs, si la CNIL ne dispose pas d'antennes déconcentrées, elle s'appuie, pour l'exercice de ses missions, sur **un réseau de correspondants informatique et libertés** au sein des entreprises et des collectivités territoriales.

Comme l'a précisé M. Alex Türk, président de la CNIL, lors de son audition par votre commission le 5 novembre 2008, ces correspondants, au nombre de **4.350**, représentent une **garantie** pour les organismes concernés et une **aide** pour l'élaboration et l'inventaire de leurs traitements de données. Ajoutons que ces correspondants ne coûtent rien à la CNIL.

Enfin, la CNIL souhaite **franchir une étape supplémentaire** en créant des antennes régionales faisant partie intégrante de l'institution.

Toutefois, ces réponses n'exonèrent pas d'une réflexion sur la simplification de la procédure d'autorisation, afin notamment qu'elle prenne en compte la différence de nature entre le projet d'un petit commerçant souhaitant s'équiper d'une caméra et celui d'une communauté d'agglomération se dotant d'un réseau complet de vidéosurveillance de la voie publique.

Recommandation n° 1 – Réunir sous une seule autorité, la CNIL, les compétences d'autorisation et de contrôle en matière de vidéosurveillance.

B. MIEUX PROTÉGER ET INFORMER LE PUBLIC

Si dans un sondage IPSOS précité 71 % des sondés se déclaraient favorables à la présence de caméras de vidéosurveillance dans les lieux publics, 79 % se déclaraient dans le même temps attachés à ce qu'un organisme indépendant contrôle ces dispositifs de vidéosurveillance pour garantir le respect du droit à la vie privée.

La tolérance de la population vis-à-vis de la vidéosurveillance n'est donc pas inconditionnelle.

Pour préserver cet équilibre au moment où la vidéosurveillance connaît un essor important, il semble nécessaire de conforter ce capital de confiance.

Le transfert à la CNIL de la compétence pour autoriser et contrôler tous les systèmes de vidéosurveillance constituerait sans aucun doute un signe fort pour rassurer nos concitoyens. D'autres mesures complémentaires sont aussi souhaitables.

1. Mieux notifier les sites au public

Le décret n° 2006-929 du 28 juillet 2006 a précisé les exigences en matière d'information du public quant à la présence d'un système de vidéosurveillance et à l'identité du responsable.

Il prévoit notamment pour les systèmes de vidéosurveillance filmant la voie publique l'utilisation de panonceaux sur lesquels une caméra est représentée. Ces prescriptions importantes restent néanmoins à mettre en œuvre dans de nombreux cas. En outre, les dispositifs mobiles devraient également faire l'objet d'une signalétique grâce à l'installation de panneaux mobiles temporaires.

Vos co-rapporteurs estiment que des dispositifs complémentaires de notification pourraient être mis à la disposition du public.

Le décret n° 96-926 du 17 octobre 1996 dispose déjà que l'autorité préfectorale met à la disposition du public la liste des autorisations publiées. Cette liste est également communiquée au maire qui la met à son tour à la disposition du public.

Cette information pourrait être utilement complétée, en particulier pour les systèmes de vidéosurveillance de la voie publique, par **la mise en ligne de cartes indiquant les zones placées sous vidéosurveillance**[1].

Enfin, chaque année, un rapport d'activité de l'ensemble des systèmes de vidéosurveillance présents sur le territoire d'une commune ou d'un établissement public de coopération intercommunale pourrait être présenté au conseil municipal ou au conseil communautaire.

Enfin, **la mention de l'enregistrement des images et de leur durée effective de conservation mériterait certainement de figurer sur les panneaux d'information**.

Recommandation n° 2 – Mieux notifier les sites au public :

- par une signalisation effective sur la voie publique ;

- par la mise en ligne de cartes indiquant les zones de la voie publique placées sous vidéosurveillance ;

- par la présentation chaque année d'un rapport d'activité de l'ensemble des systèmes de vidéosurveillance au conseil municipal ou au conseil communautaire ;

- par la mention de la durée de conservation des images sur les panneaux signalant un système de vidéosurveillance.

2. Ne pas déléguer la vidéosurveillance de la voie publique

Lors de son audition, M. Alain Bauer, président de la commission nationale de la vidéosurveillance, s'est déclaré opposé aux projets de la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur afin de permettre à des personnes privées d'assurer les missions de visionnage des images de la voie publique et d'alerte des forces de sécurité intérieure compétentes en cas de survenance d'un incident.

Il a estimé que ce type de mesure risquerait de remettre en cause la confiance du public dans la vidéosurveillance.

En outre, vos rapporteurs rappellent le principe dégagé par le juge administratif selon lequel il est impossible de déléguer une mission de police à une personne privée par un contrat.

---

[1] *Cette cartographie servirait également aux policiers et gendarmes pour vérifier rapidement si une infraction a été commise dans une zone filmée.*

Le Conseil d'Etat a précisé dans un arrêt de principe du 29 décembre 1997[1] que la surveillance de la voie publique relevait des pouvoirs de police du maire et qu'aucune délégation n'était possible. En l'espèce, un maire souhaitait confier à une société de surveillance et de gardiennage la surveillance de sa ville en soirée. Incidemment néanmoins, le juge administratif validait la possibilité de déléguer la surveillance et le gardiennage des installations et bâtiments publics à une société privée[2]. En effet, seule la surveillance de la voie publique proprement dite relève des pouvoirs de police du maire[3].

Un jugement du tribunal administratif de Nice du 22 décembre 2006[4] a fait application de cette jurisprudence à la vidéosurveillance en estimant qu'il n'y avait pas de différence de nature entre la surveillance de la voie publique et la vidéosurveillance de celle-ci, ces deux missions relevant de la mission de police municipale.

Vos co-rapporteurs estiment également que la vidéosurveillance de la voie publique à des fins de police[5] ne peut faire l'objet de délégation à des personnes privées pour les raisons exposées ci-dessus, et en raison des risques pour les libertés publiques[6].

Au surplus, il n'apparaît pas possible que des villes puissent vendre des prestations de vidéosurveillance de la voie publique à des personnes privées, en particulier à des commerçants[7].

Recommandation n° 3 – Ne pas déléguer la vidéosurveillance de la voie publique à des personnes privées, ni permettre aux autorités publiques de vendre des prestations de vidéosurveillance de la voie publique à des personnes privées.

3. Professionnaliser les opérateurs qui visionnent les images

L'expérience de la Communauté d'agglomération de la vallée de Montmorency (CAVAM) est riche d'enseignements. Le projet de vidéosurveillance comportait un volet spécifique pour la formation des opérateurs vidéo. La CAVAM a donc été amené à élaborer un projet de formation avec le concours du Centre national de la fonction publique territoriale et de la ville de Lyon.

---

[1] CE, 29 décembre 1997, commune d'Ostricourt.
[2] A cet égard, voir également CE, 20 mars 1998, SEM de sécurité active et de télématique.
[3] Art. L.2212-2 du code général des collectivités territoriales.
[4] TA de Nice, 22 décembre 2006, SA Vigitel-commune de Fréjus.
[5] Dans le cas où un système de vidéosurveillance de la voie publique aurait exclusivement des finalités étrangères aux missions de police du maire, cette jurisprudence ne s'appliquerait pas. Toutefois, en pratique, cette situation est peu vraisemblable, compte tenu en particulier de l'imbrication des finalités qui rend difficile les dissociations juridiques.
[6] Ceci n'empêche pas le recours à des partenariats public-privé pour mettre en œuvre les systèmes.
[7] A Londres, les commerçants participent au financement du système de vidéosurveillance.

Cette formation a duré un mois et avait notamment pour objectif de sensibiliser les opérateurs aux risques liés à l'utilisation de la vidéosurveillance par rapport aux libertés publiques.

En outre, M. Luc Strehaiano, président de la CAVAM, a indiqué que par mesure de sécurité les opérateurs devaient laisser leur téléphone portable à l'extérieur du centre de supervision et qu'ils étaient filmés.

L'expérience anglaise peut également être une source d'idée. Lors de la visite du centre de supervision de l'un des arrondissements de Londres (Hackney Control Center), les responsables ont expliqué à vos co-rapporteurs que lors du recrutement des opérateurs, ceux-ci faisaient l'objet d'une enquête administrative et devaient être habilités par une agence gouvernementale.

A l'avenir, pour les systèmes de vidéosurveillance de la voie publique, il conviendrait de rendre obligatoire :

- la formation des opérateurs vidéo ;

- leur habilitation ;

- leur surveillance par une caméra dans le centre de supervision.

Sur ce dernier point, vos co-rapporteurs observent que le report des images vers les services de police et de gendarmerie a pour effet de placer les opérateurs municipaux sous leur contrôle et contribue à éviter d'éventuelles utilisations abusives.

Ajoutons enfin que les policiers et gendarmes doivent aussi recevoir une formation adaptée.

Recommandation n° 4 – Former, professionnaliser et habiliter les opérateurs chargés de visionner les images de la voie publique.

4. Faut-il interdire la vidéosurveillance intelligente ?

Comme il a été vu, les systèmes de vidéosurveillance biométriques ou intelligents, c'est-à-dire permettant de programmer a priori les types de comportement à identifier, sont appelés à se développer. Cette prévision plaide d'ailleurs en faveur de la compétence de la CNIL.

Toutefois, cette garantie au regard des libertés individuelles est-elle suffisante ou faut-il aller plus loin en interdisant ces systèmes de vidéosurveillance ?

Vos co-rapporteurs sont partagés. Sans aller jusqu'à les interdire de manière absolue, il appartiendrait à la CNIL de développer une jurisprudence respectueuse du principe de proportionnalité, sur le modèle de celle qu'elle a élaborée pour le recours à la biométrie comme moyen d'identification.

Une autre solution serait de préciser dans la loi les finalités et les conditions permettant le recours à de tels systèmes. Elles seraient plus restrictives que celles applicables aux systèmes de vidéosurveillance classiques.

Recommandation n° 5 – Ne pas interdire a priori les systèmes de vidéosurveillance « intelligente », mais les soumettre à des conditions plus strictes sous le contrôle de la CNIL.

C. CRÉER LES CONDITIONS D'UN SYSTÈME DE VIDÉOSURVEILLANCE EFFICACE

1. La vidéosurveillance dans les espaces publics est-elle efficace pour lutter contre la délinquance ?

Comme le reconnaît l'INHES, la réponse à cette question n'est pas évidente, même si le ministère de l'intérieur semble avoir plus de certitudes.

Encore aujourd'hui, des évaluations solides manquent en France ce qui ne laisse pas d'étonner. Les principales études citées ont été réalisées au Royaume-Uni ou au Québec.

L'INHES pointe les difficultés pour trouver des critères et des indicateurs pertinents qui permettraient d'isoler le facteur « vidéosurveillance » parmi tous ceux qui peuvent expliquer des variations de la délinquance.

Si un jugement définitif sur l'efficacité de la vidéosurveillance ne peut être prononcé à ce stade, il est néanmoins possible de tracer quelques pistes.

Vos co-rapporteurs estiment que beaucoup de malentendus sur l'efficacité de la vidéosurveillance s'expliquent par le fait que cette technique a été perçue abusivement comme un instrument efficace de prévention situationnelle[1].

Or, les études disponibles semblent indiquer que la vidéosurveillance n'a qu'un faible impact sur la délinquance dans **les espaces complexes et étendus**. Les vols à la tire ou une agression dans une foule sont difficiles à détecter rapidement par un opérateur et, même dans cette éventualité, il lui sera difficile de suivre à la trace la fuite du délinquant.

---

[1] *Le concept de **prévention situationnelle** recouvre une série de politiques et d'actions qui, en jouant sur la rationalité du délinquant potentiel, vise à rendre difficile, risquée ou inintéressante la commission d'une infraction. **La prévention situationnelle agit sur l'environnement physique** en intégrant la prise en considération des motifs et des intentions des auteurs d'infractions et de leur perception des circonstances propices.*
Elle peut jouer :
- sur le comportement des victimes potentielles en les sensibilisant aux risques de délinquance ;
- sur l'attractivité des cibles (gardiennage, alarme, blindage, protection des cartes bancaires, projection d'encre indélébile sur les billets, neutralisation des téléphones mobiles volés...) ;
- sur l'environnement physique (vidéosurveillance, éclairage public, urbanisme permettant l'intervention des forces de sécurité...) ;
- sur la disponibilité de facilitateurs (alcool, possession d'armes ou de chiens dangereux...).

En revanche, de l'avis de tous les personnes entendues, la vidéosurveillance est efficace dans les espaces clos et offrant peu d'issues comme les parkings ou les centres commerciaux.

Surtout, la vidéosurveillance n'a qu'un faible impact sur les infractions non préméditées. Elle ne permet de dissuader que les infractions préméditées, l'auteur s'étant au préalable assuré de la présence de caméras.

Et même dans le cas de certaines infractions prémédités, l'impact n'est pas toujours avéré. Les attaques de bijouteries, toutes placées sous vidéosurveillance, en sont une illustration.

D'autres critiques portent sur les effets de report de la délinquance vers les zones non placées sous vidéosurveillance. S'ils existent certainement –en particulier pour le trafic de stupéfiants et la prostitution-, vos rapporteurs ne disposent pas de données sérieuses permettant de les mesurer.

L'effet préventif direct de la vidéosurveillance doit donc être très nuancé.

En outre, cet effet s'estompe rapidement dans le temps si la commission d'infractions sous l'œil des caméras n'est jamais suivie d'interpellations. **La prévention et la répression ne peuvent être dissociées.** La sanction est une composante essentielle de la prévention grâce à ses vertus à la fois dissuasives et pédagogiques. La lutte contre la délinquance ne peut fonctionner que si elle « *marche avec ses deux jambes* ».

Or, c'est précisément là que le bât a longtemps blessé.

Les opérateurs de vidéosurveillance sont essentiellement les collectivités territoriales et les commerces, lesquels s'attachent avant tout à prévenir la délinquance, la répression incombant exclusivement aux forces de police et de gendarmerie et à l'autorité judiciaire.

Or, le principal enseignement des travaux de vos co-rapporteurs est que la vidéosurveillance est particulièrement efficace pour la répression. C'est un outil remarquable dans la phase d'enquête et d'investigation.

Les services de police et de gendarmerie n'ont pris conscience de l'utilité de la vidéosurveillance que récemment. L'implication forte de l'Etat en faveur de cet outil ne date que de 2006-2007.

Il en a résulté que les systèmes de vidéosurveillance se sont développés en dehors de toute préoccupation de répression, la police et la gendarmerie ne bénéficiant pas du report d'images et la performance et l'implantation des caméras ne permettant pas une exploitation judiciaire des images.

L'efficacité de la vidéosurveillance en a nécessairement pâti.

L'exemple anglais témoigne de cette prise de conscience, les efforts portant désormais sur l'amélioration de la qualité des images, de la formation des agents, de l'exploitation des images et des partenariats entre tous les

acteurs de la sécurité. L'expérience globale de la Communauté d'agglomération de la vallée de Montmorency apporte également de bons indicateurs de l'efficacité de la vidéosurveillance pour faire baisser la délinquance de voie publique.

2. Pour un usage raisonné de la vidéosurveillance

Vos co-rapporteurs mettent en garde contre toute stigmatisation d'une technologie. La vidéosurveillance n'est ni la panacée, ni un « *big brother* ».

Du point de vue de l'efficacité, la mise en place d'un système de vidéosurveillance doit **privilégier la qualité sur la quantité**. Vos co-rapporteurs rejoignent largement l'analyse de l'INHES sur les conditions d'une exploitation efficace[1].

Cela implique impérativement :

● une phase de conception longue et approfondie.

Un diagnostic de sécurité devrait être systématiquement élaboré en collaboration avec les forces de police et de gendarmerie. Par ailleurs, les conseils locaux ou intercommunaux de sécurité et de prévention de la délinquance devraient être le cadre principal de conception du système de vidéosurveillance. Ces instances doivent déterminer clairement les objectifs poursuivis.

● des partenariats très étroits entre tous les acteurs : collectivités, services de police et de gendarmerie, commerçants, bailleurs sociaux, transporteurs…

Ce partenariat ne signifie pas la confusion des rôles. Chacun doit rester dans son champ de compétence ; en particulier les collectivités territoriales ne doivent pas connaître de la répression, mais seulement mettre leurs images à la disposition des services de police et de gendarmerie.

● une formation de **tous les acteurs** pour acquérir le réflexe d'utiliser la vidéosurveillance et apprendre à l'utiliser.

S'agissant des agents municipaux, et des opérateurs vidéo en particulier, des formations adaptées devraient être développées par le CNFPT et le recrutement devrait être perfectionné. Comme l'écrit le rapport de l'INHES, « *la vidéo protection est un véritable métier* ». A défaut, le risque est d'avoir de simples téléspectateurs devant les écrans de supervision.

● de développer les systèmes de vidéosurveillance au niveau des bassins de vie, afin notamment de limiter les effets de report de la délinquance.

---

[1] *Voir la deuxième partie du rapport précité.*

La loi autorise déjà les EPCI à prendre en charge les frais de conception, de déploiement et d'entretien de la vidéosurveillance. Une étape pourrait être franchie en transférant automatiquement cette compétence aux EPCI dès lors qu'ils exercent la compétence relative à la prévention de la délinquance.

Cette démarche plus professionnelle semble gagner du terrain. Selon M. Philippe Melchior, les premières tendances sur 2008 indiqueraient un ralentissement des nouvelles implantations au profit d'une meilleure réflexion en amont des projets et d'une meilleure évaluation a posteriori.

Vos co-rapporteurs insistent également sur le fait qu'il n'existe pas une solution idéale convenant à tous. Une caméra de qualité avec enregistrement mais sans visionnage en temps réel peut suffire dans bien des cas. Les images ne seront consultées qu'en cas de commission d'une infraction dans le cadre d'une procédure judiciaire. Ce système coûtera moins cher et posera moins de problème au regard des libertés publiques. Dans les zones rurales, ce type de système peut être particulièrement utile.

Recommandation n° 6 – Un usage raisonné de la vidéosurveillance doit être favorisé, l'accent devant porter sur la qualité des systèmes plutôt que sur la multiplication du nombre de caméras implantées. Cela suppose en particulier :

- une phase de conception longue et approfondie ;

- des partenariats très étroits entre tous les acteurs : collectivités, services de police et de gendarmerie, commerçants, bailleurs sociaux, transporteurs… Toutefois, ce partenariat ne signifie pas la confusion des rôles, chacun devant rester dans son champ de compétence ;

- une formation de tous les acteurs pour acquérir le réflexe d'utiliser la vidéosurveillance et apprendre à l'utiliser ;

- le développement des systèmes de vidéosurveillance au niveau des bassins de vie. A cet égard, cette compétence devrait être transférée automatiquement aux établissements publics de coopération intercommunale qui exercent déjà la compétence relative à la prévention de la délinquance.

D. SIMPLIER LES PROCÉDURES ET S'ADAPTER À DE NOUVELLES UTILISATIONS

1. Une procédure d'autorisation trop lourde

Le décret n° 96-926 du 17 octobre 1996 précise les pièces à fournir lors du dépôt d'une demande d'autorisation préalable à l'installation d'un système de vidéosurveillance dans les espaces publics.

Parmi la dizaine de pièces exigées, certaines sont mal aisées à fournir comme le plan masse des lieux ou un plan de détail montrant le nombre et l'implantation des caméras.

Or, le décret du 17 octobre 1996 ne fait aucune distinction entre le projet d'un petit commerçant souhaitant s'équiper d'une caméra et celui d'une communauté d'agglomération se dotant d'un réseau complet de vidéosurveillance de la voie publique.

Il serait souhaitable de réduire le nombre de documents exigés pour les systèmes les plus simples ou rudimentaires. Il y a là un gisement d'économie et de gain de temps important sans que les libertés publiques en souffrent.

Par ailleurs, plutôt que de délivrer une autorisation pour chaque caméra installée, **des zones vidéo surveillées** pourraient être délimitées à l'intérieur desquelles le responsable du système de vidéosurveillance serait libre de déplacer les caméras et d'en moduler le nombre dans la limite d'un plafond.

Enfin, les dossiers de renouvellement des autorisations seraient soumis à une procédure simplifiée sauf en cas de modification substantielle.

Recommandation n° 7 – Différencier le traitement administratif des demandes d'autorisation en fonction de la taille et de la nature des systèmes de vidéosurveillance. Une procédure simplifiée pourrait s'appliquer aux systèmes les plus simples dans les lieux ouverts au public.

Recommandation n° 8 – Plutôt que de délivrer une autorisation pour chaque caméra installée, des zones vidéo surveillées devraient être délimitées à l'intérieur desquelles le responsable du système de vidéosurveillance serait libre de déplacer les caméras et d'en moduler le nombre dans la limite d'un plafond.

Recommandation n° 9 – Soumettre à une procédure simplifiée les dossiers de renouvellement des autorisations, sauf en cas de modification substantielle.

2. Accepter de nouvelles finalités ?

Une première question est celle de la légalité des utilisations de la vidéosurveillance aux fins de la gestion urbaine de proximité.

Faut-il admettre la vidéosurveillance, compte tenu des risques pour la vie privée et les libertés individuelles, aux seules fins de faciliter la gestion de la voirie ou de la propreté ?

Vos rapporteurs sont réservés. La vidéosurveillance est un outil trop sensible pour être déployé par simple souci de commodité de gestion. Toutefois, la loi pourrait être aménagée pour légaliser ces utilisations à la condition qu'elles soient **accessoires** par rapport aux finalités principales fixées par la loi du 21 janvier 1995 (prévention de la délinquance, protection des bâtiments, régulation du trafic routier).

Il reviendrait à l'autorité de contrôle de s'assurer que ces utilisations sont bien accessoires.

Une seconde question porte sur les dispositifs de vidéosurveillance implantés pour une durée limitée, par exemple à l'occasion d'une manifestation ou d'un évènement culturel ou sportif présentant des risques particuliers de délinquance.

Les délais de procédure sont mal adaptés à ces utilisations. La procédure d'urgence issue de la loi du 23 janvier 2006 ne peut être actuellement utilisée qu'aux fins de prévention du terrorisme.

Une solution serait de prévoir une procédure d'urgence pour d'autres finalités que la prévention du terrorisme.

A bien des égards, un dispositif temporaire est préférable à un système permanent. Il est notamment plus conforme aux principes de finalité et de proportionnalité.

Recommandation n° 10 – Admettre d'autres finalités pour l'utilisation de la vidéosurveillance à la condition que ces finalités restent accessoires par rapport aux finalités principales que sont la prévention de la délinquance, la protection des bâtiments et la régulation du trafic routier.

Recommandation n° 11 – Faciliter le recours à des dispositifs mobiles de vidéosurveillance implantés pour une durée limitée, par exemple à l'occasion d'une manifestation ou d'un évènement culturel ou sportif présentant des risques particuliers de délinquance, de préférence à des dispositifs permanents à l'utilité variable.

*

* *

Vos co-rapporteurs se sont efforcés d'éviter de stigmatiser ou, inversement, de sacraliser la vidéosurveillance, cet outil n'étant ni incompatible avec le respect de la vie privée et des libertés individuelles, ni la réponse magique aux problèmes de délinquance.

L'expérience montre que seul un usage raisonné et réfléchi permet d'obtenir des résultats en matière de lutte contre la délinquance, dans des proportions qui restent toutefois à mieux évaluer.

Une erreur serait de n'investir que dans la multiplication du nombre de caméras, sans qu'un travail de formation, de partenariat et de concertation ne soit mené avant et après l'installation des caméras.

Vos co-rapporteurs ajoutent que chaque responsable d'un système de vidéosurveillance doit rester maître de déterminer ses besoins. L'Etat peut inciter, orienter ou conseiller, mais il ne doit pas se substituer aux autorités compétentes.

Surtout, au moment où des innovations technologiques importantes vont modifier la nature de la vidéosurveillance et accélérer encore son développement, vos co-rapporteurs estiment nécessaires de redonner une cohérence forte au cadre légal de la vidéosurveillance avant que des dérives n'apparaissent. A cet égard, la CNIL, autorité indépendante, semble la mieux placer pour assurer cette mission en lieu et place des préfets.

En effet, le débat sur la vidéosurveillance ne peut être abordé indépendamment de l'enjeu plus global du traçage des individus consécutif au développement exponentiel des technologies de l'information. L'histoire et les compétences actuelles de la CNIL lui confèrent la vision d'ensemble nécessaire pour veiller à la préservation des libertés sans entraver un emploi proportionné de ces technologies.

Réunie le mercredi 10 décembre 2008, la commission a autorisé la publication du présent rapport.

ANNEXES

———

ANNEXE 1

LISTE DES PERSONNES ENTENDUES

Inspection générale de l'administration

M. Philippe Melchior, inspecteur général de l'administration, président du Comité de pilotage stratégique de la vidéosurveillance au ministère de l'intérieur

Police nationale

M. Frédéric Péchenard, directeur général de la police nationale

M. Winter, conseiller pour la vidéoprotection

Gendarmerie nationale

Général d'armée Guy Parayre, directeur général de la gendarmerie nationale

Lieutenant-Colonel Haurtault

Commission nationale de la vidéosurveillance

M. Alain Bauer, président

Commission nationale de l'informatique et des libertés

M. Alex Türk, président

Mme Sophie Vuillet-Tavernier, directrice des affaires juridiques, internationales et de l'expertise

Association des Maires de France

M. Luc Strehaiano, président de la communauté d'agglomération de la vallée de Montmorency

Universitaire

M. Frédéric Ocqueteau, universitaire et chercheur au CNRS

Commission nationale consultative des droits de l'homme

M. Joël Thoraval, président

Mme Isabelle Delise

Ligue des droits de l'homme

M. Alain Weber, référent vidéosurveillance

M. Jean-Claude Vitran, responsable de la commission Libertés et Informatique

ANNEXE 2

DÉPLACEMENTS DU GROUPE DU TRAVAIL

Visite du PC sécurité de la RATP (quai de la Râpée, Paris 75012) le mardi 8 juillet 2008

- présentation du dispositif de sécurité sur le réseau de la RATP et de l'utilisation de la vidéosurveillance

- visite des deux salles de contrôle, l'une gérée par les agents de la RATP, l'autre par la police nationale

Visite du Technocentre Orange à Châtillon (92) le mercredi 23 juillet 2008

- présentation de la vision d'Orange sur la vidéosurveillance : de la caméra analogique avec stockage local à la caméra IP avec stockage centralisé qui permet la mutualisation des usages

- démonstration sur la vidéo intelligente et la reconnaissance des visages, axes de recherche des « Orange Labs »

- visite du showroom sur les derniers produits et services Orange pour les clients résidentiels

Déplacement à Londres

Mardi 9 septembre 2008

- Départ du Sénat à 7 h – arrivée à Londres à 9 h 34

- 11h : accueil au Central Communications Command Centre (109 Lambeth Road) de la Metropolitan Police.

→ Présentation de la « Special Operations Room »

→ Présentation des aspects techniques de la vidéosurveillance (CCTV) par M. Ian Cunningham du ministère de l'intérieur (Home Office)

→ Présentation de la vidéosurveillance comme moyen d'investigation judiciaire par l'inspecteur chef Mick Neville

→ Présentation des utilisations de la vidéosurveillance en matière d'ordre public et en cas d'incident grave par l'inspecteur Sam Simpson

→ Visite de la salle de contrôle. Démonstration.

- 13h : Déjeuner buffet et questions

- 14h30 : Rencontre au Home Office avec les équipes du « Research Directorate », le centre d'étude, d'évaluation et d'analyse du ministère.

- 16h : Rendez-vous téléphonique avec M. Jonathan Bamford « Deputy Information Commissioner » de la commission de contrôle « Information Commissioner » (la CNIL britannique située près de Manchester).

- 17h30 : Retour à l'hôtel

Mercredi 10 septembre 2008

- 9h : Départ de l'hôtel

- 9h30 : Visite du Hackney control centre avec M. Andy Wells, deputy service manager (184, Stok Newington, Church Street- London- N16 OJR), centre local de supervision de la vidéosurveillance dans l'un des quartiers de Londresgéré par une société privée sous-traitante.

- 12h30 : Départ de Londres – Arrivée à Paris : 15h50

ANNEXE 3
EXTRAITS DE LA LOI N°95-73 DU 21 JANVIER 1995 D'ORIENTATION ET DE PROGRAMMATION RELATIVE À LA SÉCURITÉ

Article 10
Modifié par loi n°2006-64 du 23 janvier 2006 -
art. 1 JORF 24 janvier 2006

I. - Les enregistrements visuels de vidéosurveillance répondant aux conditions fixées au II sont soumis aux dispositions ci-après, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

II. - La transmission et l'enregistrement d'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 la protection des bâtiments et installations publics et de leurs abords, la sauvegarde des installations utiles à la défense nationale, la régulation du trafic routier, la constatation des infractions aux règles de la circulation ou la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression ou de vol.

La même faculté est ouverte aux autorités publiques aux fins de prévention d'actes de terrorisme ainsi que, pour la protection des abords immédiats de leurs bâtiments et installations, aux autres personnes morales, dans les lieux susceptibles d'être exposés à des actes de terrorisme.

Il peut être également procédé à ces opérations dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol ou sont susceptibles d'être exposés à des actes de terrorisme.

Les opérations de vidéosurveillance de la voie publique sont réalisées de telle sorte qu'elles ne visualisent pas les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées.

Le public est informé de manière claire et permanente de l'existence du système de vidéosurveillance et de l'autorité ou de la personne responsable.

III. - L'installation d'un système de vidéosurveillance dans le cadre du présent article est subordonnée à une autorisation du représentant de l'Etat dans le département et, à Paris, du préfet de police, donnée, sauf en matière de défense nationale, après avis d'une commission départementale présidée par un magistrat du siège ou un magistrat honoraire.

L'autorisation préfectorale prescrit 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.

L'autorisation peut prescrire que les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales sont destinataires des images et enregistrements. Elle précise alors les modalités de transmission des images et d'accès aux enregistrements ainsi que la durée de conservation des images, dans la limite d'un mois à compter de cette transmission ou de cet accès, sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale. La décision de permettre aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales d'être destinataires des images et enregistrements peut également être prise à tout moment, après avis de la commission départementale, par arrêté préfectoral. Ce dernier précise alors les modalités de transmission des images et d'accès aux enregistrements. Lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, cette décision peut être prise sans avis préalable de la commission départementale. Le président de la commission est immédiatement informé de cette décision qui fait l'objet d'un examen lors de la plus prochaine réunion de la commission.

Les systèmes de vidéosurveillance installés doivent être conformes à des normes techniques définies par arrêté ministériel, à compter de l'expiration d'un délai de deux ans après la publication de l'acte définissant ces normes.

Les systèmes de vidéosurveillance sont autorisés pour une durée de cinq ans renouvelable.

La commission départementale instituée au premier alinéa peut à tout moment exercer, sauf en matière de défense nationale, un contrôle sur les conditions de fonctionnement des dispositifs autorisés en application des mêmes dispositions. Elle émet, le cas échéant, des recommandations et propose la suspension des dispositifs lorsqu'elle constate qu'il en est fait un usage anormal ou non conforme à leur autorisation.

Les autorisations mentionnées au présent III et délivrées antérieurement à la date de publication de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers sont réputées délivrées pour une durée de cinq ans à compter de cette date.

III bis. - Lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent délivrer aux personnes mentionnées au II, sans avis préalable de la commission départementale, une autorisation provisoire d'installation d'un système de vidéosurveillance, exploité dans les conditions prévues par le présent article, pour une durée maximale de quatre mois. Le président de la commission est immédiatement

informé de cette décision. Il peut alors la réunir sans délai afin qu'elle donne un avis sur la mise en œuvre de la procédure d'autorisation provisoire.

Le représentant de l'Etat dans le département et, à Paris, le préfet de police recueillent l'avis de la commission départementale sur la mise en œuvre du système de vidéosurveillance conformément à la procédure prévue au III et se prononcent sur son maintien. La commission doit rendre son avis avant l'expiration du délai de validité de l'autorisation provisoire.

IV. - Hormis le cas d'une enquête de flagrant délit, d'une enquête préliminaire ou d'une information judiciaire, les enregistrements sont détruits dans un délai maximum fixé par l'autorisation. Ce délai ne peut excéder un mois.

V. - Toute personne intéressée peut s'adresser au responsable d'un système de vidéosurveillance afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans le délai prévu. Cet accès est de droit. Un refus d'accès peut toutefois être opposé pour un motif tenant à la sûreté de l'Etat, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou au droit des tiers.

Toute personne intéressée peut saisir la commission départementale mentionnée au III de toute difficulté tenant au fonctionnement d'un système de vidéosurveillance.

Les dispositions du précédent alinéa ne font pas obstacle au droit de la personne intéressée de saisir la juridiction compétente, au besoin en la forme du référé.

VI. - Le fait d'installer un système de vidéosurveillance ou de le maintenir sans autorisation, de procéder à des enregistrements de vidéosurveillance sans autorisation, de ne pas les détruire dans le délai prévu, de les falsifier, d'entraver l'action de la commission départementale, de faire accéder des personnes non habilitées aux images ou d'utiliser ces images à d'autres fins que celles pour lesquelles elles sont autorisées est puni de trois ans d'emprisonnement et de 45000 euros d'amende, sans préjudice des dispositions des articles 226-1 du code pénal et L. 120-2, L. 121-8 et L. 432-2-1 du code du travail.

VI bis. - Le Gouvernement transmet chaque année à la Commission nationale de l'informatique et des libertés un rapport faisant état de l'activité des commissions départementales visées au III et des conditions d'application du présent article.

VII. - Un décret en Conseil d'Etat fixe les modalités d'application du présent article et notamment les conditions dans lesquelles le public est informé de l'existence d'un dispositif de vidéosurveillance ainsi que de l'identité de l'autorité ou de la personne responsable. Ce décret fixe également les conditions dans lesquelles les agents visés au III sont habilités à accéder

aux enregistrements et les conditions dans lesquelles la commission départementale exerce son contrôle.

Article 10-1

Créé par Loi n°2006-64 du 23 janvier 2006 - art. 2 JORF 24 janvier 2006

I. - Aux fins de prévention d'actes de terrorisme, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent prescrire la mise en œuvre, dans un délai qu'ils fixent, de systèmes de vidéosurveillance, aux personnes suivantes :

- les exploitants des établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ;

- les gestionnaires d'infrastructures, les autorités et personnes exploitant des transports collectifs, relevant de l'activité de transport intérieur régie par la loi n° 82-1153 du 30 décembre 1982 d'orientation des transports intérieurs ;

- les exploitants d'aéroports qui, n'étant pas visés aux deux alinéas précédents, sont ouverts au trafic international.

II. - Préalablement à leur décision et sauf en matière de défense nationale, le représentant de l'Etat dans le département et, à Paris, le préfet de police saisissent pour avis la commission départementale instituée à l'article 10 quand cette décision porte sur une installation de vidéosurveillance filmant la voie publique ou des lieux et établissements ouverts au public.

Les systèmes de vidéosurveillance installés en application du présent article sont soumis aux dispositions des quatrième et cinquième alinéas du II, des deuxième, troisième, quatrième et sixième alinéas du III, du IV, du V, du VI et du VII de l'article 10.

III. - Lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, le représentant de l'Etat dans le département et, à Paris, le préfet de police peuvent prescrire, sans avis préalable de la commission départementale, la mise en œuvre d'un système de vidéosurveillance exploité dans les conditions prévues par le II du présent article. Quand cette décision porte sur une installation de vidéosurveillance filmant la voie publique ou des lieux ou établissements ouverts au public, le président de la commission est immédiatement informé de cette décision. Il peut alors la réunir sans délai afin qu'elle donne un avis sur la mise en œuvre de la procédure de décision provisoire.

Avant l'expiration d'un délai maximal de quatre mois, le représentant de l'Etat dans le département et, à Paris, le préfet de police recueillent l'avis de la commission départementale sur la mise en œuvre du système de vidéosurveillance conformément à la procédure prévue au III de l'article 10 et se prononcent sur son maintien.

IV. - Si les personnes mentionnées au I refusent de mettre en oeuvre le système de vidéosurveillance prescrit, le représentant de l'Etat dans le département et, à Paris, le préfet de police les mettent en demeure de procéder à cette installation dans le délai qu'ils fixent en tenant compte des contraintes particulières liées à l'exploitation des établissements, installations et ouvrages et, le cas échéant, de l'urgence.

V. - Est puni d'une amende de 150 000 Euros le fait, pour les personnes mentionnées au I, de ne pas avoir pris les mesures d'installation du système de vidéosurveillance prescrit à l'expiration du délai défini par la mise en demeure mentionnée au IV.