European Forum *for* Urban Security

Citoyens, villes et vidéosurveillance

Quel est le prix à payer pour une société où la sécurité serait une valeur absolue ? Saturer l'espace de caméras heurte notre droit à l'anonymat. L'autorité publique a un devoir d'en justifier la levée. La Convention européenne des droits de l'Homme nous invite à exiger des réponses. Il nous semble indispensable que les modalités d'emploi des caméras et des images soient précisées. ➤

Cofinancé par la Commission européenne
Programme sur les droits fondamentaux
et la citoyenneté

European Forum *for* Urban Security

Citoyens, villes et vidéosurveillance

Vers une utilisation démocratique et responsable de la vidéosurveillance

Cette publication est le fruit de la collaboration de tous les partenaires du projet « Citoyens, villes et vidéosurveillance ». Elle a été éditée par le Forum européen pour la Sécurité urbaine, Roxana Calfa, Sebastian Sperber et Nathalie Bourgeois.

Traduction : Helga Birkle, Jara Campelo, Charlotte Combe, Kerstin Elsner, Nathalie Elson, Mariapia Falcone, Gianfranca Gabbai, John Tyler Tuttle.

Conception graphique : Pete Jeffs, Marie Aumont

Achevé d'imprimer en juin 2010
par STIPA - Montreuil
N°ISBN : 2-913181-37-6
N°EAN : 9782913181373

European Forum for Urban Security
10 rue des Montibœufs, 75020 Paris, France
Tél : + 33 (0) 1 40 64 49 00
fax : + 33 (0) 1 40 64 49 10
www.efus.eu
contact@efus.eu

Le projet « Citoyens, villes et vidéosurveillance » ainsi que cette publication ont été réalisés grâce au financement de la Commission européenne/direction générale Justice, Liberté et Sécurité/ programme Droits fondamentaux et Citoyenneté.

Remerciements
Ce projet et cette publication n'auraient pas été possibles sans l'implication des représentants des partenaires du projet, des villes, régions et autorités de police. Nous les remercions chaleureusement pour avoir fait vivre ce projet.
Nous remercions aussi en particulier les experts pour leur contribution importante à cet ouvrage, les hôtes des diverses réunions, visites d'études et de la conférence finale, de même que tous ceux et celles que nous avons eu le plaisir de rencontrer et écouter tout au long de ce projet.

Partenaires du projet :
Catherine Schlitz, Christian Beaupere, Guy Geraerts, Serge Lodrini (Liège, Belgique), Bertrand Binctin, Christophe Bois (Le Havre, France), Charles Gautier, Dominique Talledec, Eric Fossembas (Saint-Herblain, France), Rossella Selmini, Gian Guido Nobili (Emilie-Romagne, Italie), Francesco Scidone, Mariapia Verdona, Marcelo Sasso, Marco Morelli (Gênes, Italie), Giorgio Vigo (Vénétie, Italie), Ahmed Aboutaleb, Ineke Nierstrazs, Afke Besselink, Niels Witterholt, Nienke Riemersma, Wilco Mastenbroek, Linda Ouwerling, Ciska Scheidel (Rotterdam, Pays-Bas), Manuel Ayala Garcia, Juan-Jose Ferrer Planells, Tomas Paris (Ibiza, Espagne), Christopher Ambler, Roger Fox (police du Sussex, Royaume-Uni), Andrew Bayes, James Farrell (police métropolitaine de Londres, Royaume-Uni).

Partenaires associés :
Stanislav Jaburek, Lenka Stepankova (Brno, République tchèque), Béla Danielisz, Gabor Gulyas, Zoltan Nemeth, Krisztina Szego (Budapest, Hongrie).

Experts :
Benjamin Goold (université d'Oxford Royaume-Uni/ université de Colombie-Britannique, Canada), Jeroen Van Den Hoven (université technique de Delft, Pays-Bas), Laurent Lim (CNIL, France), Maye Seck (Forum français pour la Sécurité urbaine), Peter Squires (université de Brighton, Royaume-Uni), Eric Töpfer (université technique de Berlin, Allemagne).

Autres intervenants/personnalités rencontrées :
Alessandra Risso, Gianluca Saba, Yuri Piccione, Rinaldo Sironi, Valerio Piazzi, Piero Anchini, Amerigo Alunno, Dario Messina, Furio Truzz (Gênes, Italie), Graeme Gerrad, Brian Watkinson, Dave Hinton, Ken Crawley, Mick Neville, Isabella Sankey, (Londres/Brighton, Royaume-Uni), Isabelle Mercier, Didier Delorme, Emmanuel Magne, Georges Pasini, Louis-Jean Despres, M. Pareja, Jacques Signourel, Patrick Aujogue, Thierry Dussauze, Jacques Comby (Lyon, France), József Schmidt, Attila Cserép, Richárd Schranz, Péter Rózsas, Endre Szabo, Tivadar Hüttl, Tomáš Koníček, Klára Svobodová (Budapest, Hongrie), R.V. de Mulder, Laurie Bush, Zsuzsanna Belényessy, Sylvie Murengerantwari, Caroline Atas (Rotterdam, Pays-Bas).

Sommaire

Avant-propos

Les villes se densifient ; elles multiplient les offres de mobilité, de culture, d'éducation faisant appel à une multiplicité d'équipements de plus en plus complexes dont les coûts de fonctionnement sont élevés. Les flux de circulation se croisent, le *show off* de l'offre marchande s'étale aux yeux et aux appétits du public. La surveillance humaine 24h sur 24 devient impossible pour des raisons de coûts, mais le développement de l'électronique dans la capitalisation des informations et leur croisement, dans la fourniture d'outils se voulant préventifs ou dissuasifs, poussent à la multiplication des caméras installées dans les espaces dédiés aux transports, aux réunions de foule, aux lieux d'exposition de la marchandise ou d'objets de grande valeur financière. La prévention des incidents techniques est prédominante dans cette mise en place de caméras, dont les images sont à la fois regardées en direct et aussi, de plus en plus souvent, analysées par des logiciels. La préservation de l'intégrité des équipements est la seconde priorité de ces installations ; le mauvais usage et la dégradation volontaire demandent des interventions rapides pour certains équipements dont le fonctionnement peut concerner des milliers de personnes. Une compensation à la réduction des effectifs humains en charge

du fonctionnement d'un équipement est la troisième motivation à ces installations. Cet ensemble de motifs fait de nos villes des consommatrices d'images de surveillance. Les utilisateurs de ces images appartiennent à la sphère privée comme à la sphère publique.

Mais un quatrième motif est apparu donnant au débat une vive tournure politique. On peut arrêter grâce aux caméras des délinquants opérant sur la voie publique, dans les espaces publics. Ce motif est né d'un constat négatif porté sur l'efficience des services de police. Augmenter le taux d'élucidation devrait permettre aussi de diminuer les velléités du délinquant de passer à l'acte. Cet axiome d'une criminologie de tendance libérale pose le principe que si l'on augmente chez le délinquant la conscience de la certitude qu'il se fera prendre, il renoncera à son dessein. D'où ce double argument utilisé dans les textes officiels : les caméras vidéo contribuent à la prévention de la délinquance et servent à arrêter les délinquants. Peut être, peut être… Le jeu en vaut-il la chandelle ? Les études ne montrent pas de façon nette une diminution de la délinquance ; elles enregistrent des arrestations dans quelques cas criminels justifiant des enquêtes approfondies, mais l'effet de masse attendu n'est pas au rendez-vous. Un rendez-vous placé sous le signe de l'inquiétude. Pour atteindre au moins le deuxième objectif et encore plus le premier, il faut mettre des caméras partout dans la ville car les crimes sont assez également répartis sur le territoire urbain. A partir de ce seuil, consistant à saturer l'espace public de caméras, nous basculons dans une société de méfiance, de restriction des libertés. Le débat s'engage.

Quel prix voulons-nous payer pour une société plaçant la sécurité comme une valeur absolue ? Un rapport parlementaire français vient d'être publié suite à une série de catastrophes naturelles. Sa conclusion principale est de s'interroger sur la nécessité de réintroduire une culture du risque chez les citoyens. Le triomphalisme de la technologie a éliminé de la conscience du citoyen la notion de risque. Que faire pour lui dire que malgré la technologie, il doit continuer de savoir qu'il est en situation de risque ? N'est-ce pas la même question qu'on devrait se poser à propos de la délinquance ? Il n'y a pas de société sûre, sans délinquance et tout moyen proposé qui se veut éliminatoire du risque devrait être rejeté par les citoyens responsables.

Saturer l'espace public de multiples caméras heurte notre droit à l'anonymat. L'Autorité publique a un devoir de justifier la levée de cet anonymat. La Convention européenne des droits de l'Homme nous y invite, mais il nous semble indispensable que les modalités de l'emploi des caméras et des images soient précisées. Tel est l'objet du travail effectué par des praticiens et des experts sous l'égide du Forum.

Michel Marcus
Délégué général du Forum européen
pour la Sécurité urbaine

Introduction

La vidéosurveillance à la hausse

La première décennie du XXIème siècle a commencé sous le signe d'un événement qui aura marqué les esprits et les pratiques. Les attentats du 11 septembre 2001 ont imposé la sécurité comme priorité sur l'agenda mondial. Depuis, une pléthore de moyens considérés utiles dans la lutte contre le terrorisme, dont la vidéosurveillance, a été déployée à tous les niveaux. Les questions de leur efficacité, de l'adéquation entre les objectifs visés et les instruments utilisés et de leur impact, surtout à long terme, sur les libertés ont été secondaires.

Des attentats terroristes ont été commis bien avant 2001, mais ils n'avaient pas atteint cette dimension globale mise en exergue par les médias. Ce n'est pas un hasard si l'Etat européen qui en a fait l'expérience de manière régulière et prolongée – le Royaume-Uni – est celui qui a le plus cherché a développer toutes les réponses possibles autant en termes de prévention que de résilience.

Le choix de la technologie pour faire face à la demande croissante de sécurité de la part des citoyens a trouvé sa justification dans les événements du 11 septembre 2001, au même titre que ceux du 11 mars 2004 à Madrid et du 7 juillet 2005 à Londres. Le recours à la technologie n'a cessé de croître depuis dans tous les autres pays européens.

Or, comme les images impressionnantes présentées seulement quelques heures après les attentats de Londres montrant comment les présumés terroristes sont arrivés sur le lieu du crime, l'intervention en 2008 du responsable de la vidéosurveillance à Londres la qualifiant de fiasco a fait le tour du monde. Une fois l'émotion des événements passée, il conve-

nait de s'interroger sur la pertinence de l'utilisation de la technologie dans les actions de prévention, sur son efficacité, et également sur les avantages et les inconvénients qui découlent de son usage.

Ces interrogations sont d'actualité autant dans les pays qui envisagent de recourir à plus de vidéosurveillance, comme la France l'a décidé en 2008, que dans ceux qui sont déjà très avancés dans l'utilisation de cette technologie, comme le Royaume-Uni. Depuis 25 ans, le Royaume-Uni a connu un essor exponentiel de ces technologies et il est aujourd'hui le leader mondial de l'utilisation de la vidéosurveillance. Cependant, depuis quelques années, de nombreuses voix se sont élevées pour remettre en question le bien-fondé du « tout-vidéosurveillance » et pour tirer les leçons de l'expérience. Les Britanniques mènent aujourd'hui une réflexion sur leurs systèmes et en particulier la façon de les utiliser[1]. Ainsi, le nouveau vice-Premier ministre, Nick Clegg, a annoncé récemment que le gouvernement allait préparer une nouvelle loi de protection des droits fondamentaux. Il déclarait, dans une conférence de presse le 19 mai 2010 : « Ce gouvernement va mettre un terme a cette culture d'intrusion dans la vie privée de ses citoyens. Il est inacceptable que des personnes qui respectent la loi soient traitées comme si elles avaient quelque chose à cacher…La vidéosurveillance va faire l'objet de lois sur mesure…»[2].

Ces interrogations deviennent d'autant plus d'actualité pour les villes européennes que la technologie s'invite dans l'élaboration des politiques locales et régionales de sécurité. Les élus locaux doivent à la fois répondre aux demandes de sécurité de leurs habitants et justifier le choix des instruments qu'ils mettent en place, dans un souci de transparence et d'exercice démocratique du processus de prise de décision. En admettant que la technologie soit la réponse considérée comme la plus appropriée par les Etats pour lutter contre des menaces tel le terrorisme, qu'en est-il au niveau local pour la prévention de la criminalité ? La plupart des villes et régions européennes sont confrontées à une délinquance de tous les jours, qui n'a pas d'effets aussi spectaculaires que ceux d'une attaque terroriste, mais qui néanmoins remet en cause le bien-vivre ensemble sur un territoire et peut nuire au développement durable de celui-ci. Elles sont donc amenées à considérer tout instrument qui peut les aider à garantir la sécurité de leurs citoyens et ne peuvent ignorer les atouts potentiels de la technologie.

S'il est vrai que les citoyens donnent comme mandat aux élus d'assurer leur sécurité, ils les investissent également de leur confiance, afin que les choix de sécurité ne se fassent pas au détriment du respect des droits et libertés garantis par la loi. Cette confiance suppose aussi que les autorités assument la responsabilité du choix et de l'utilisation transparente des instruments employés aux fins de sécurité.

Droit à la sécurité, droit à la protection de sa vie pri-vée ? Y a-t-il un ordre de priorité ? Est-ce que l'un prévaut sur l'autre ? En théorie, les citoyens devraient pouvoir jouir des deux sans avoir à choisir entre l'un ou l'autre. Les deux vont de pair dans une société démocratique et ils sont garantis à parts égales autant par les cadres législatifs nationaux que par les textes internationaux comme la Convention des droits de l'Homme du Conseil de l'Europe (1950) ou la Charte des Droits fondamentaux de l'Union européenne (2000). Or, dans la pratique, la conciliation entre sécurité et libertés est loin d'être évidente. La liberté est

[1] Stratégie nationale pour la vidéosurveillance, 2008
[2] DEPUTY PRIME MINISTER – SPEECH AND Q&A – 19/05/2010, London

un droit faible, qui est facilement relativisé face aux problématiques d'insécurité. La vidéosurveillance est une technologie qui soulève beaucoup de questions dans ce sens. Que peut-on filmer ? Y a-t-il un droit à la vie privée dans l'espace public ? Et si oui, comment protéger ce droit ? Comment éviter de discriminer certains groupes et comment mettre les avantages de cet outil de surveillance à la disposition de toute la population ? Comment faire pour que la vidéosurveillance marche et quand recourir à d'autres instruments ? Quand est-elle efficace dans un rapport coûts-bénéfices ? Comment protéger les données personnelles et comment ne pas les produire inutilement ? Comment utiliser la vidéosurveillance avec les citoyens en tant qu'outil de prévention de la criminalité et de garantie de la tranquillité publique ?

Une réflexion et un échange d'expériences sur les pratiques de la vidéosurveillance dans le respect et la protection des libertés individuelles

C'est pour répondre à toutes ces questions et identifier les bonnes pratiques que ce projet européen « Citoyens, villes et vidéosurveillance » a vu le jour. Cette réflexion a pu être développée grâce à l'implication de dix partenaires, à savoir les villes du Havre et de Saint-Herblain (France), Rotterdam (Pays-Bas), Liège (Belgique), Ibiza (Espagne), Gênes, les régions de Vénétie et Emilie-Romagne (Italie), les polices de Londres et Sussex (Royaume-Uni), ainsi que des experts européens. Le projet a reçu le soutien financier de la Commission européenne (programme Droits fondamentaux et citoyenneté).

Le projet visait à donner aux villes les connaissances et les outils nécessaires à la mise en place d'une politique de sécurité intégrée où les réalités sociales et les libertés sont prises en compte au même titre que la tranquillité publique.

Pour répondre aux défis posés par la vidéosurveillance en termes de droits et libertés, les partenaires se sont fixés comme objectif spécifique d'approfondir la question fondamentale de la responsabilité de l'élu local qui doit trouver un équilibre entre la demande de sécurité et les choix stratégiques lui permettant d'y répondre de manière démocratique.

Comme l'indique l'intitulé du projet, les citoyens sont au coeur des politiques locales. A ce titre, il fallait donc porter une attention particulière à la prise en compte des citoyens lors de la mise en place ou de l'évaluation des dispositifs de vidéosurveillance. En effet, dans la mesure où ces dispositifs sont destinés avant tout à servir les citoyens, ceux-ci devraient être non seulement consultés sur leurs attentes et besoins en termes de sécurité mais aussi parfaitement informés sur le fonctionnement, les coûts et les bénéfices de ces nouveaux outils. Les partenaires ont donc examiné comment prendre en compte ces questions à toutes les étapes de mise en oeuvre d'un projet de vidéosurveillance, depuis l'installation, le fonctionnement jusqu'à son évaluation, et ils ont débattu et proposé des solutions alternatives ou complémentaires. De plus, ce partenariat de villes, régions, polices municipales et régionales, s'est donné comme ambition de formuler une *Charte pour une utilisation démocratique de la vidéosurveillance*, c'est-à-dire dans le respect des droits fondamentaux. L'objectif à terme est de mettre en œuvre cette charte et de définir un label qui identifie les villes respectant ses principes et ses recommandations.

L'idée sous-jacente de cette démarche conjointe est aussi d'établir un langage commun sur la vidéosur-

veillance en Europe, accessible et compréhensible pour tous. Il s'agit d'une démarche nécessaire pour assurer la transparence des processus de décisions politiques.

Les villes aident les villes…

La méthodologie du projet est fondée sur la mission fondamentale du Forum européen pour la sécurité urbaine : « Les villes aident les villes ». Les villes, régions et autorités de police souhaitaient améliorer leur système en partageant leurs expériences et en en tirant les enseignements. Cet échange a été enrichi et complété par les contributions d'experts comme le Forum français pour la Sécurité urbaine et un certain nombre de professeurs de grandes universités et hauts fonctionnaires, qui ont permis d'enrichir la réflexion et de faire le lien entre recherche et pratiques. Les expériences de chacun des partenaires ont été analysées selon une grille de lecture. Ces échanges de pratiques et de savoir-faire se sont concrétisés sous la forme de la *Charte pour une utilisation démocratique de la vidéosurveillance*.

… pour créer dans le cadre d'une coopération européenne une charte pour une utilisation démocratique de la vidéosurveillance.

Dès la réunion de démarrage du projet, tenue à Paris en avril 2009, la richesse des expériences et la diversité des situations présentées par les partenaires sont apparues. Diversité technique tout d'abord, avec des différences notables autant en ce qui concerne le nombre de caméras (de quatre à 60.000 !), que le type de caméras et leur fonctionnalité, que la couverture géographique. Diversité aussi des contextes politiques : quelles autorités peuvent décider d'installer des caméras sur l'espace public, quels opérateurs peuvent en être les gestionnaires, quelles sont les personnes autorisées à transmettre les informations et celles qui peuvent en être destinataires, quel cadre légal, quels débats sur la vidéosurveillance au niveau national et local (voir partie III de cette publication). Diversité aussi en termes de lisibilité et de perception de la vidéosurveillance pour les citoyens des villes partenaires du projet : favorable chez les uns, méfiance et réserves chez les autres, ce qui induit différents niveaux de débat public autour de l'utilisation des caméras et la protection des droits fondamentaux. Diversité des situations et des législations enfin, qui a mis en évidence la difficulté de s'accorder sur le champ d'application du projet : vidéosurveillance dans l'espace public uniquement ? Comment traiter les espaces semi-publics, les espaces privés à usage public ? L'approche retenue était de se concentrer sur l'espace public pour lequel tous les partenaires sont compétents, sans pour autant perdre de vue les systèmes de vidéosurveillance de l'espace semi-public qui représentent une très grande partie des systèmes existants et pour lesquelles les conclusions du projet pourraient également être source d'inspiration.

Le premier objectif du projet était d'avoir une vue d'ensemble des pratiques de la vidéosurveillance et des mesures prises pour protéger la vie privée des citoyens. Les grilles de lecture des pratiques des partenaires du projet ont permis de voir comment la protection des données était intégrée dans les différentes phases de la vie d'un système de vidéosurveillance, à savoir l'analyse des besoins, l'installation, la gestion et l'évaluation.

Pour compléter cette vue d'ensemble et pour avoir une compréhension commune de la problématique, les partenaires du projet ont bénéficié, dès le premier séminaire de travail qui a eu lieu au Havre les 3 et 4

juin 2009, de l'apport des experts issus de différentes filières, juridique, politique/sociologique, technique, philosophique et des représentants des ONG de protection des droits de l'homme et des associations de police.

Experts et professionnels étaient d'accord sur les principaux défis de la vidéosurveillance dans les espaces publics, qui seraient :

➤ d'une part, de trouver une manière de préserver les codes sociaux de l'intimité dans l'espace public dans un cadre vidéosurveillé. Cette thématique est développée dans cet ouvrage par Benjamin Goold. Elle est également présente dans la jurisprudence de la Cour européenne des Droits de l'Homme de Strasbourg portant sur les plaintes contre les « paparazzi » ;

➤ d'autre part, de trouver un bon équilibre en termes de rapport coûts-bénéfices entre le prix que les gens sont prêts à payer en renonçant jusqu'à un certain point à leur intimité et les bénéfices qu'ils obtiennent grâce à une sécurité accrue. Ce qui voudrait dire que les décisions se prendraient en toute conscience et en toute connaissance des effets.

➤ Les manquements au respect de son intimité ne sont pas perçus par le citoyen comme étant très importants. Cependant, en fin de compte, la somme de chaque petite intrusion dans la vie privée d'un citoyen peut prendre des proportions considérables et cette tendance est décuplée à chaque développement technologique. La protection de la vie privée dans l'espace public relève de l'autorité politique et les acteurs concernés devraient être associés à cette démarche. Il fallait donc prendre en compte la protection des données et des libertés individuelles à chaque niveau d'utilisation de la vidéosurveillance.

Dans un deuxième temps le projet a permis de voir en détail des pratiques de la vidéosurveillance lors de visites in-situ organisées par trois partenaires du pro-jet : la ville de Gênes (Italie), la police métropolitaine de Londres et la police du Sussex (Royaume-Uni) et Lyon (France), ville associée au projet.

Ces visites ont d'abord permis d'obtenir des connaissances détaillées sur l'utilisation de la vidéosurveillance, de voir sur le terrain la manière dont est géré un système et d'échanger avec diverses parties prenantes sur les problèmes et les atouts de cette technologie.

La visite d'étude à Londres et Brighton a notamment permis d'obtenir des informations sur l'expérience anglaise de la vidéosurveillance, intégrée comme instrument d'investigation dans la criminologie, et de prendre connaissance des débats qui ont cours au Royaume-Uni sur son impact sur la vie privée, grâce aux rencontres avec des experts employés par le gouvernement dans la lutte anti-terroriste et des militants d'ONG comme Liberty.

La visite à Gênes a illustré la réalité d'une ville italienne dans laquelle plusieurs systèmes de vidéosurveillance opèrent, sous la direction d'institutions différentes. Ici, le défi est le partage de l'information : jusqu'où et dans quelles conditions ?

La visite à Lyon a notamment permis de comprendre la démarche d'une ville qui avait déjà accompagné son système de vidéosurveillance d'une charte éthique et qui avait aussi mis en place un collège éthique chargé de superviser le système.

Ces visites d'étude ont également montré comment les villes et les régions utilisent de manière différente

la vidéosurveillance, par rapport aux objectifs qu'elles poursuivent, et en quoi varient également les protocoles de gestion, la communication, la relation caméras publiques-caméras privées, et l'attitude des citoyens, entre soutien et opposition. Il est clairement apparu que l'impact de la vidéosurveillance varie selon la nature et la taille des espaces surveillés, le type de délit, l'association de cette technologie ou non avec d'autres mesures de prévention.

Ces visites ont également permis d'identifier un certain nombre de dispositifs et mesures mis en place afin de garantir la protection de la vie privée des citoyens, entre autres le paramétrage spécial des caméras, la formation des opérateurs sur le cadre légal régissant la protection des données, les chartes de « bon usage » où les villes s'engagent à respecter les droits fondamentaux, et les systèmes de supervision indépendante.

L'éclairage apporté par les experts, les visites de sites, les rencontres avec des professionnels locaux, les grilles de lecture décrivant les pratiques des partenaires ont par la suite servi de base de discussions pour les deux séminaires de travail qui se sont tenus à Budapest, les 2 et 3 décembre 2009 et à Bologne, les 11 et 12 mars 2010.

Le séminaire de Budapest a d'abord été l'occasion d'inclure des pratiques de l'Europe centrale dans le projet, avec des contributions et des visites de la ville de Budapest, de l'ombudsman pour la protection de données et des ONG hongroises et des contributions de la ville de Brno (République Tchèque) et du ministère tchèque de l'Intérieur. Le séminaire a aussi permis d'illustrer la difficulté de trouver un langage commun qui reflète les problématiques variées à travers l'Europe, de passer outre les clivages politiques pour arriver à un dénominateur commun qui ne soit pas simplement un accord a minima des positions des partenaires. Par exemple la notion d'une charte « éthique » très acceptée en France n'a pas fait l'unanimité au niveau européen. La solution retenue d'une charte pour une « utilisation démocratique » de la vidéosurveillance, traduisait le mieux l'esprit du projet qui met les citoyens au cœur des politiques locales dans un souci d'exercice démocratique du pouvoir de représentativité des élus. Le choix entre les notions de « vidéo-protection » ou « vidéosurveillance » a été aussi largement débattu.

Les débats ont également tourné autour de la création d'un label pour la mise en œuvre de la charte. Ce label serait destiné aux villes qui respectent ses principes. Les avis étaient également mitigés : tandis que certains y voyaient d'emblée la continuation logique d'un travail pour la mise en œuvre de la charte, d'autres étaient plus réservés à l'idée de se faire auditionner pour recevoir ce label. Ceci dit, il n'était pas prévu de réaliser un label dans le cadre de ce projet, mais seulement d'en étudier la faisabilité.

Le séminaire de Bologne a servi à identifier les principes clés de la charte, déclinés à chaque phase de vie du système. Le défi était de trouver des principes indépendants mais complémentaires qui caractérisent ensemble une utilisation démocratique de la vidéosurveillance.

Il a été également l'occasion de proposer une initiative allant vers la création d'un langage commun de la vidéosurveillance à travers l'Europe : la création d'une signalétique commune, standardisée, qui puisse transmettre un message clair et complet à n'importe quel citoyen à travers l'Europe. Plusieurs discussions ont porté sur les informations indispensables qu'une

telle signalétique devrait comporter, à la lumière de ce qui existe déjà dans les villes et pays représentés dans le projet.

La définition des sept principes fédérateurs qui sont au coeur de la *Charte pour une utilisation démocratique de la vidéosurveillance* ainsi que les commentaires d'explication qui les accompagnent ont été rédigés par les partenaires lors d'un travail en commun, lors d'un ultime séminaire qui a eu lieu à Paris le 9 avril 2010.

La conférence finale du projet, accueillie par la ville de Rotterdam les 27 et 28 mai 2010, a marqué à la fois l'aboutissement de 18 mois de travail des partenaires et la reconnaissance de la responsabilité des élus quant à l'utilisation de la vidéosurveillance. En devenant les premiers signataires de la charte, les maires de Rotterdam, Ahmed Aboutaleb et de Saint-Herblain, Charles Gautier, également sénateur et président du Forum français pour la sécurité urbaine, ont ainsi réaffirmé que les élus locaux sont responsables devant les citoyens des outils qu'ils choisissent pour mettre en oeuvre leur politique, et qu'ils ont également une obligation de transparence. Les deux édiles ont par ailleurs invité les autres villes européennes à signer la charte.

Cette publication est donc le reflet de ce long travail, qui a permis aux dix partenaires européens du projet de partager les points de vue d'experts provenant de divers pays d'Europe, d'échanger des pratiques expérimentées par les villes, de débattre des enjeux et défis de la vidéosurveillance au regard du respect de la vie privée et enfin de formuler ensemble des propositions de réponses.

Partie I

➤ *Le défi : concilier l'utilisation de la vidéosurveillance avec les libertés individuelles*

Vidéosurveillance et droits de l'Homme

Benjamin J. Goold
Université de Colombie-Britannique (Canada)/
Université d'Oxford (Royaume-Uni)

Ces vingt dernières années, l'utilisation des caméras de vidéosurveillance est devenue de plus en plus courante en Europe. Bien que certains pays comme la France, l'Allemagne, la Hollande et l'Italie aient tardé à suivre l'exemple de la Grande-Bretagne, des systèmes de vidéosurveillance sont maintenant installés dans de nombreuses villes du continent européen, de telle sorte que la surveillance des espaces publics est devenue une réalité inévitable de la vie pour un nombre croissant d'européens. Bien que le public semble fortement appuyer l'utilisation de la vidéosurveillance, la propagation de cette technologie a de sérieuses conséquences sur les libertés individuelles et la relation entre les citoyens et l'Etat. En particulier, les caméras de vidéosurveillance représentent une menace importante pour la vie privée et l'exercice de droits tels que la liberté d'expression et la liberté d'association. En conséquence, il est vital que les personnes responsables de la gestion et de l'exploitation de ces systèmes soient conscientes des dangers de la surveillance des espaces publics et qu'elles œuvrent à garantir que les droits fondamentaux de l'homme ne soient en aucun cas menacés par cette vidéosurveillance.

Ce chapitre donne un bref aperçu des implications de la vidéosurveillance sur les droits fondamentaux des citoyens et vise à assister les responsables et exploitants de cette technologie dans le développement des politiques et des pratiques de surveillance des espaces publics en accord avec un engagement de protection des droits individuels et de respect des libertés civiles.

Vidéosurveillance et vie privée

Le respect d'un minimum de vie privée doit être assuré pour tout un chacun. Sans cela, il serait impossible de conserver sa dignité, de développer de vraies relations ou simplement de prendre le temps de se noyer dans ses pensées. La vie privée est vitale à notre développement parce qu'elle nous libère du souci d'être constamment observé et jugé par ceux qui nous entourent. Ceci nous permet de contrôler la façon et le moment où nous partageons des informations nous concernant avec d'autres. C'est pour ces raisons que la majorité des pays reconnaissent au moins certains droits élémentaires à la vie privée et limite le droit des individus, des organismes privés et de l'Etat de collecter des informations sur la vie personnelle ou de surveiller des personnes sans leur consentement et à leur insu.[2]

Il est important de reconnaître que le droit à la vie privée ne s'arrête pas dès que nous franchissons le seuil de nos maisons. Bien qu'aucune personne sensée ne puisse s'attendre à bénéficier du même niveau de confidentialité dans la rue que dans son propre salon, la plupart d'entre nous s'attendent à jouir d'un certain degré de confidentialité et d'anonymat lorsque nous sortons en public. En effet, une des choses les plus agréables de la vie en ville est la possibilité de se perdre dans la foule et d'être libéré des contraintes familiales, des amis ou des collègues. C'est en partie cette promesse d'anonymat et de liberté associée à la vie citadine qui attire de nombreuses personnes en ville. De même, bien que peu de personnes s'attendent à rencontrer un ami dans un restaurant ou un café et être complètement libres de toute attention, il existe de fortes conventions sociales qui nous permettent de profiter d'un niveau d'anonymat satisfaisant dans ces circonstances. Bien que notre anonymat ne soit pas aussi manifeste dans les espaces publics qu'il ne l'est dans notre sphère

privée qu'est la maison ou la voiture, il est clair que nous avons droit à un certain respect de notre vie privée dans l'espace public.[3]

De par sa nature, la vidéosurveillance de ces espaces publics remet en cause ce droit. En nous exposant à la surveillance à chaque fois que nous marchons dans la rue, les caméras nous dépouillent de tout anonymat vis-à-vis d'un Etat vigilant. Alors que nous abandonnons une grande partie de notre anonymat à chaque fois que nous sortons dans un lieu public, le fait que les autres membres du public nous observent également ne doit pas être une justification pour les utilisateurs de vidéosurveillance. Etre observé et probablement filmé par une caméra de vidéosurveillance est un acte différent de celui d'être observé par un étranger. Le premier type d'observation est typiquement plus long, plus intense et plus intimement lié au pouvoir en place. Parce que nous ne voyons ni ne questionnons la personne derrière la caméra, il nous est difficile de savoir quelle réponse donner à la vidéosurveillance ou de décider ce que nous devons en faire. Parce que nous ne savons pas si les images enregistrées par les caméras seront conservées ou qui pourrait y accéder, nous ne savons

[1] Pour un aperçu des différentes théories sur la vie privée, consulter : Solove, D.J. (2002), "Conceptualizing Privacy", *California Law Review* 90: 1087-1155; Solove, D.J. (2009) *Understanding Privacy* (Harvard University Press: Cambridge, Mass.); et Nissenbaum, H. (2010), *Privacy in Context* (Stanford University Press: Stanford, Californie).

[2] Une des déclarations les plus pertinentes de ces droits est donné par l'Article 8 de la Convention européenne des droits de l'Homme : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »

[3] Voir : **Goold, B.J.** (2002), "Privacy Rights and Public Spaces: CCTV and the Problem of the 'Unobservable Observer'", *Criminal Justice Ethics* 21(1) Winter/Spring; et Goold, B.J. (2008) "The Difference between Lonely Old Ladies and CCTV Cameras: A Response to Jesper Ryberg", *Res Publica* (March).

pas si elles seront mal interprétées ou utilisées de façon contestable. Comme le dit le philosophe et criminologue Andrew von Hirsch, une surveillance par caméra s'apparente à *effectuer ses activités quotidiennes devant un miroir sans tain, tout en sachant qu'une personne se trouve probablement derrière le miroir, sans vraiment savoir qui est cette personne, ni ce qu'elle recherche.*[4]

Mis à part l'intrusion évidente, c'est l'incertitude engendrée par les caméras de vidéosurveillance qui représente une des plus grande menaces pour notre anonymat dans les espaces publics. Face à la perspective d'une vidéosurveillance constante, il est raisonnable de s'attendre à ce que certains membres du public ressentent fortement la perte d'anonymat et modifient leur comportement, non parce qu'ils pensent faire quelque chose d'illégal, mais parce qu'ils ne veulent pas attirer l'attention de la police ou risquer d'avoir leurs actions mal interprétées. Ceci est probablement vrai pour les jeunes et pour certaines minorités qui pourraient se sentir injustement ciblés par la police et les autorités locales. Comme le déclare Giovanni Buttarelli, Contrôleur européen adjoint de la Protection des données :

Le fait d'être observé modifie notre comportement. En effet, être observé peut amener chacun de nous à censurer son discours et sa conduite. C'est certainement le cas avec une surveillance extensive ou en continu. La surveillance de chacun de nos déplacements et de nos gestes peut avoir un impact psychologique et modifier nos comportements. Ceci constitue une atteinte à notre vie privée.[5]

Comment les exploitants et les responsables de réseaux de vidéosurveillance s'assurent-ils que la surveillance de l'espace public ne remette en cause le

droit à la vie privée ou ne modifie de façon négative la façon dont le public profite des espaces publics ? Tout d'abord, il est crucial que de tels systèmes soient exploités conformément à la législation locale ou nationale. Tous les efforts doivent être faits pour éviter les utilisations abusives des images et les failles de sécurité du système. Ensuite, les caméras ne devraient être utilisées qu'aux fins identifiées à l'origine lorsque la décision de les installer a été prise : la modification incontrôlée des utilisations doit être évitée. Enfin, les systèmes doivent être ouverts et transparents, et les responsables d'exploitation doivent rendre des comptes au public. Alors que l'installation de caméras de vidéosurveillance dans les espaces publics aura inévitablement un impact négatif sur la vie privée des individus, en s'assurant que les mesures mentionnées ci-dessus soit mises en place, les exploitants et responsables de réseaux de vidéosurveillance peuvent contribuer à minimiser la perte d'anonymat et s'assurer que la surveillance est adéquate et légale.

Caméras de vidéosurveillance, liberté d'expression et liberté d'association

Même s'il est évident que les caméras de vidéosurveillance ont un grave impact sur la vie privée, l'utilisation de technologie de surveillance de l'espace public par la police et les autorités locales peut remettre

[4] **von Hirsch**, A. (2000), "The Ethics of Public Television Surveillance" in von Hirsch, A., Garland, D. and Wakefield, A. (eds.) *Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing: Oxford)

[5] « Restrictions juridiques – la Surveillance et les Droits Fondamentaux, Discours par **Giovanni Buttarelli**, Contrôleur Européen Adjoint de la Protection des Données au Palais de Justice, Vienne, le 19 juin 2009 (disponible sur : *www.edps.europa.eu/…site/…/09-06-19_Vienna_surveillance_EN.pdf)*

en cause certains autres droits fondamentaux. En particulier, les caméras de vidéosurveillance peuvent décourager le public d'exercer son droit à la liberté d'expression et à la liberté d'association dans un lieu public. Ces dernières représentent deux droits essentiels à l'idée d'une autonomie démocratique et doivent être protégées pour permettre aux individus qui le souhaitent de former des organisations politiques, de critiquer les décisions de leurs élus et de demander des comptes au gouvernement. Si les citoyens savent qu'ils risquent d'être filmés à chaque fois qu'ils assistent à un rassemblement public ou qu'ils participent à une manifestation, il existe un danger très réel que la présence des caméras de vidéosurveillance ait un effet néfaste sur l'expression de ces droits, conduisant éventuellement à une réduction des libertés politiques et de la participation démocratique. Cette possibilité a d'ailleurs été récemment reconnue par le département de la Sécurité Intérieure aux Etats-Unis dans une étude de l'impact sur la vie privée des systèmes de vidéosurveillance exploités par le service américain de l'Immigration et des Douanes.

Les caméras de vidéosurveillance fournissent au gouvernement des informations sur ce que la population dit, fait ou lit dans les espaces publics, par exemple en documentant les personnes présentes à une manifestation particulière ou les associations entre individus. Ceci pourrait décourager l'expression et les associations protégées par la constitution.[7]

Etant donné la menace potentielle sur la liberté d'expression et d'association, il est vital que la vidéosurveillance soit uniquement utilisée pour prévenir la criminalité et encourager la sécurité publique et jamais dans le but de rassembler des informations sur les opinions ou activités politiques des citoyens.

Lorsque, par exemple, la police envisage d'utiliser la vidéosurveillance pour surveiller une manifestation, dans le but de maintenir l'ordre et d'éviter toute violence, elle doit veiller à ne pas conserver des images d'individus sauf si celles-ci seront utilisées comme preuves dans une enquête criminelle. De même, lorsque des images d'une personne sont enregistrées dans le but de la poursuivre en justice pour un délit, ces images ne doivent pas être ensuite transmises aux services de sécurité ou autres agences du maintien de l'ordre sauf en cas de raisons incontestables de le faire.

En plus de ces restrictions, la police et les autres utilisateurs de la vidéosurveillance des espaces publics doivent faire en sorte que le public soit parfaitement informé des objectifs, du fonctionnement de ces systèmes ainsi que des règlementations auxquelles ils doivent obéir. Si les effets néfastes de la vidéosurveillance doivent être évités, la restriction de l'utilisation de la vidéosurveillance ainsi que l'adoption de mesures de protection de la vie privée ne sont pas suffisantes. Le public doit être certain que les systèmes ne seront pas utilisés à mauvais escient et qu'avec le temps, ils ne seront pas utilisés à des fins politiques. Ceci est particulièrement important dans les pays qui n'ont que récemment fait la transition

[7] Département de la Sécurité Intérieure aux Etats-Unis, *Privacy Impact Assessment for the Livewave CCTV System* (17 septembre 2009). Cette remarque a également été faite par Buttarelli qui déclare : « La vidéosurveillance peut décourager les comportements légitimes tels que les manifestations politiques qui soutiennent des causes impopulaires. Traditionnellement, les participants ont le droit de participer anonymement à un rassemblement pacifique, sans risque d'identification ou de répercussions. Ceci est en train de changer fondamentalement ». Voir « Restrictions juridiques – la Surveillance et les Droits Fondamentaux », Discours par Giovanni Buttarelli, Contrôleur Européen Adjoint de la Protection des Données au Palais de Justice, Vienne, le 19 juin 2009, p. 8.

vers un régime démocratique et où les souvenirs de répression politique sont encore frais dans les mémoires. Il est très difficile pour la police et l'Etat de gagner la confiance du public mais très facile de la perdre. Une utilisation abusive de la vidéosurveillance pour des raisons politiques ou autres non légitimes pourrait gravement ébranler cette confiance.

Concilier sécurité et droits

Il y a, en effet, des circonstances où il est tout à fait légitime et nécessaire de sacrifier, dans une certaine mesure, la vie privée et autres droits fondamentaux dans l'intérêt de la sécurité. Notre société doit pouvoir se défendre de la meilleure façon qu'il soit face aux menaces. Toutefois, la charge de la preuve doit toujours être supportée par ceux qui prétendent que de tels sacrifices sont nécessaires et que les mesures proposées sont toutes efficaces pour la protection de la société. [8]

Une des interrogxlance dans les espaces publics (rues, centres-villes) puissent avoir un impact significatif sur la réduction des délits et du désordre public, elles peuvent également être une menace sérieuse pour les droits individuels et politiques. En conséquence, il est vital que la police et autres utilisateurs de la vidéosurveillance gardent à l'esprit les points suivants lorsqu'ils utilisent une méthode de surveillance des espaces publics :

➤ *La vidéosurveillance empiète inévitablement sur les droits à la vie privée d'un individu*

En conséquence, la police et les autorités locales doivent s'assurer qu'elles ont des raisons légales et convaincantes pour justifier de l'utilisation de la vidéosurveillance dans un lieu public et qu'elles ont mis en place des systèmes de contrôle et de responsabilité qui tentent de minimiser les impacts négatifs

de la surveillance sur la vie privée d'une personne.

➤ *La vidéosurveillance constitue une menace sérieuse pour l'exercice de la liberté politique*

La surveillance des espaces publics et des manifestations, lorsqu'elle est appuyée par l'Etat, peut potentiellement et sérieusement remettre en cause la capacité et la volonté des individus à exercer leurs droits de liberté d'expression et d'association. De ce fait, la vidéosurveillance ne doit jamais être utilisée dans le but de rassembler des informations sur les activités ou affiliations politiques des citoyens. Les utilisateurs de vidéosurveillance doivent pouvoir garantir que les caméras de vidéosurveillance ne seront jamais utilisées à des fins politiques ou pour décourager les réunions ou manifestations publiques.

➤ *Le public doit être certain que les exploitants de la vidéosurveillance respecteront ses droits*

Avant tout, le public doit être certain que les exploitants de la vidéosurveillance respecteront ses droits. Cette confiance doit être justifiée. Même si la vidéosurveillance n'est pas utilisée à mauvais escient, si le public pense que ces droits sont bafoués, la présence des caméras risque de remettre en cause la confiance obtenue par la police et l'Etat. Les utilisateurs de la vidéosurveillance ne doivent pas seulement respecter les droits individuels, le public doit également être certain qu'ils se sont engagés à protéger la vie privée et à respecter les droits à la liberté d'expression et d'association.

[8] « Restrictions juridiques – la Surveillance et les Droits Fondamentaux, Discours par **Giovanni Buttarelli**, Contrôleur Européen Adjoint de la Protection des Données au Palais de Justice, Vienne, le 19 juin 2009, p.4 (disponible sur : www.edps.europa.eu/.../site/.../09-06-19_Vienna_surveillance_EN.pdf)

L'exploitation de systèmes de vidéosurveillance dans les espaces publics exige que la police et autres organismes publics prennent en compte l'un des dilemmes les plus fondamentaux de nos sociétés démocratiques modernes : la compétition entre la demande de sécurité et notre engagement commun pour la protection des droits individuels. Si la police et les autres organismes publics envisagent de concilier ces deux objectifs, ils doivent d'abord reconnaître que c'est à l'Etat de justifier de la surveillance des citoyens et non aux citoyens d'expliquer pourquoi ils ne doivent pas être surveillés. Dès que cette vérité fondamentale se perd, ce n'est qu'une question de temps avant que les droits ne soient menacés par la surveillance.

Evaluation de la vidéosurveillance : enseignements d'une culture de surveillance

Peter Squires, *université de Brighton (Royaume-Uni)*

La prolifération de la vidéosurveillance au Royaume-Uni permet aux autres sociétés d'en savoir davantage. Pour certains, cette affirmation pourrait être un point de départ un peu trop controversé. Comme l'a argumenté Marianne L. Gras dans son article publié en 2004 « The Legal Regulation of CCTV in Europe », alors que la Grande-Bretagne a probablement servi d'exemple quant à l'ampleur de son investissement dans la vidéosurveillance, certains autres commentateurs ne sont pas convaincus que les mécanismes britanniques de contrôle juridique et politique ne soient pas distancés ou que le modèle britannique soit même à suivre.

Ces vingt dernières années, le gouvernement britannique a été un des leaders mondiaux de l'investissement en vidéosurveillance. Le ministère de l'Intérieur britannique a récemment estimé : « A bien des égards, nous avons servi d'exemple au reste du monde depuis l'introduction de la vidéosurveillance dans les années 70 jusqu'au développement exponentiel de l'installation et de l'exploitation de cette technologie dans les années 90 ». Entre 1999 et 2003, un total de 170 millions de livres sterling (environ 200 millions d'euros en 2010) pour le financement de la vidéosurveillance ont été mis à la disposition des autorités locales à la suite d'un processus d'appels d'offres. Il en a résulté plus de 680 projets de vidéosurveillance, installés dans les centres villes et autres lieux publics dans toute la Grande-Bretagne.

Il est compréhensible qu'avec le déploiement rapide d'une technologie peu testée, de nombreuses erreurs ont été faites. Petit à petit mais pas toujours de manière aisée, certaines leçons sur les résultats et les limitations de la vidéosurveillance ont été tirées. Benjamin Goold, maître de conférence à la faculté de droit de l'Université de Colombie-Britannique et ancien enseignant à Oxford, est allé jusqu'à remarquer qu'en 2004, bien que le gouvernement soit prêt à financer le développement de nouveaux systèmes de vidéosurveillance dans de nombreuses villes britanniques, « celui-ci ne semblait pas manifester un intérêt particulier de savoir si ces systèmes fonctionnaient réellement ». En conséquence, les installations de systèmes de vidéosurveillance se sont multipliées en Grande-Bretagne, probablement de façon plus rapide que nécessaire, à en juger par le manque de preuves de leur efficacité ou de leur impact. En effet, la vidéosurveillance semble avoir eu un impact négligeable sur le taux de criminalité dans les zones où elle a été installée. Pourtant, l'attente totalement irréaliste que la vidéosurveillance pourrait résoudre de nombreux problèmes de criminalité et de désordre dans les lieux publics a persisté. Celle-ci a été partiellement favorisée par la collaboration contre nature entre des entrepreneurs de police enthousiastes, des commerciaux de l'industrie de la sécurité et des citoyens craintifs.

Comme l'a conclu une étude de 2005 effectuée pour le Ministère de l'Intérieur : *Les mérites de [la vidéosurveillance] comme réponse à tous les problèmes de criminalité ont été exagérés – et ce par les gouvernements successifs. Rares étaient ceux qui, cherchant à partager les fonds mis à disposition, ont cru bon de démontrer l'efficacité de la vidéosurveillance... Pourtant, dans certaines circonstances, celle-ci semblait rarement la meilleure réponse aux problèmes de criminalité.*

Au fur et à mesure que les autres pays augmentent leurs investissements en vidéosurveillance, il est possible de tirer des leçons utiles de l'expérience du Royaume-Uni et d'améliorer les processus de transfert de politiques, d'éviter les erreurs, de développer de meilleures pratiques, de clarifier certains problèmes et même de réduire les coûts. Il est également possible de développer des politiques basées sur des preuves. Dans un domaine d'élaboration des politiques publiques qui opposent la puissance de l'Etat et la sécurité à la vie privée du citoyen et aux droits individuels, les problématiques autour de la gestion, la gouvernance et le contrôle des systèmes de vidéosurveillance en Grande-Bretagne peuvent être une base utile à partir de laquelle les autres sociétés peuvent établir les leurs. Alors que le Forum européen pour la Sécurité urbaine s'oriente vers le développement d'un code européen de bonnes pratiques et d'éthique pour la vidéosurveillance, l'expérience britannique peut être une leçon salutaire. Au sens large, ceci confirme une réalité déplaisante sur les politiques d'ordre public. Comme David Garland le dit dans son livre de 2001 *The culture of control*,

« les stratégies de contrôle de la criminalité...ne sont pas adoptées parce qu'elles sont reconnues comme solution aux problèmes. Les politiques et les stratégies sont souvent adoptées parce qu'elles sont politiquement rapides, populaires, peu coûteuses, en accord avec les priorités existantes ou favorisées par les intérêts dominants. »

Comme le remarque Stephen Savage (professeur de Criminologie et directeur de l'Institut d'études sur la Justice Pénale, université de Portsmouth), les politiques et l'idéologie plutôt que la recherche ont modelé la majorité des politiques d'ordre public des années 90. Il est aussi vraisemblable d'argumenter que

les différents appels à projet de la vidéosurveillance organisés par le ministère de l'Intérieur depuis les années 90 – et la forme qu'ils ont pris avec des offres de financement public/privé – avaient autant pour but la relance des partenariats locaux de prévention de la criminalité que le financement de la vidéosurveillance. Il est discutable que l'industrie de la vidéosurveillance au Royaume-Uni ait bénéficié de façon spectaculaire d'un concours de circonstances unique et de son habile publicité. Nous procéderons peut-être différemment la prochaine fois.

A une époque où les menaces perçues (crime, violence, émeutes et terrorisme) génèrent des exigences de sécurité plus importantes et où les industries de la sécurité détectent des nouveaux marchés lucratifs, le milieu de la recherche devrait faire deux choses. D'une part, veiller à ce que les mesures adoptées pour la prévention de la criminalité permettent d'obtenir les réductions promises. D'autre part, veiller à ce que ces mesures ne deviennent pas des méthodes coûteuses d'intensification des politiques d'ordre public déjà tendues et souvent dysfonctionnelles. Par exemple, les politiques qui aboutissent à accentuer les pouvoirs de la police vis-à-vis des droits des citoyens, ou renforcer les frontières sociales problématiques entre de supposés « innocents » citoyens et les « autres ». Cela peut être aussi des politiques qui diabolisent les jeunes et autres groupes de publics « visibles », en finançant la sécurité des nantis et en redistribuant (c'est à dire en déplaçant) les risques criminels vers des communautés déjà vulnérables, donc en facilitant l'émergence d'un ordre public moins opposé au risque et, au final, moins redevable.

L'auteur français et commentateur social Loïc Wacquant a catalogué de tels développements aux Etats-Unis au cours des dix dernières années et met les

Européens en garde contre la tendance qui consiste à lutter contre la délinquance et les problèmes d'ordre public uniquement par la justice pénale et les mesures de sécurité. Il remarque : « toute politique qui prétend lutter contre les crimes violents uniquement par les moyens de la justice pénale se condamne d'office à l'inefficacité ...tout en aggravant les problèmes qu'elle était supposée résoudre ».

La démarche d'adoption de la vidéosurveillance au Royaume-Uni, ressemblant à la recherche de la « solution magique », associée à une vague de soutien public populiste mais mal informé, ne doit pas représenter la démarche qu'il est recommandé de suivre aveuglément. Ce n'est pas parce que la technologie n'a pas donné les résultats attendus (nombre d'entre eux étaient, de toute façon, exagérés, irréalistes et déraisonnables) mais plutôt parce que l'adoption de la vidéosurveillance amène de nombreuses autres questions sur les pratiques de maintien de l'ordre, lesquelles demandent une sérieuse réflexion pour savoir si la technologie doit être intégrée de façon efficace dans la justice pénale et les infrastructures de sécurité.

En dehors du Royaume-Uni, les citoyens et les autorités locales peuvent répondre à de telles questions de façon radicalement différente et ils peuvent vouloir utiliser la vidéosurveillance pour résoudre d'autres problèmes. Ceci, dans un sens, est le tout premier point. Nous ne devrions pas demander : que peuvent faire les caméras de vidéosurveillance pour nous ? Mais plutôt, quels problèmes souhaitons-nous résoudre et comment la vidéosurveillance peut-elle nous y aider ?

Perspectives politiques

A partir de 2007, tout en reconnaissant qu'il y a encore un « débat » sur « l'efficacité de la vidéosurveillance pour la réduction et la prévention de la criminalité », le ministère de l'Intérieur britannique et l'Association of Chief Police Officers (l'Association des Chefs de Police - ACPO) ont été suffisamment honnêtes pour reconnaître que même si la vidéosurveillance a contribué à « la protection du public et à assister la police », ceci s'est fait « malgré un développement à tâtons sans véritable direction, contrôle ou règlementation stratégique, une approche qui a empêché la maximisation du potentiel de l'infrastructure de vidéosurveillance ». Le rapport indique également que ce « développement de la vidéosurveillance sans approche organisée représente un risque important en termes de compatibilité des systèmes, de coût d'accès aux images et de perte potentielle d'efficacité opérationnelle ».

Pourtant, comme nous l'avons remarqué, au-delà de ces problématiques essentiellement opérationnelles d'utilité, d'impact et d'efficacité, de nombreuses autres questions se posent sur la démocratie, les droits, la citoyenneté, le contrôle, la responsabilité et les recours qui ont toutes un impact sur la confiance du public vis-à-vis du maintien de l'ordre. Les sociétés qui développent leurs propres systèmes de vidéosurveillance doivent tenir compte de ces problématiques et ne pas seulement se concentrer que sur les questions techniques.

Bien que la police soit maintenant prête à accepter les critiques faites par les communautés universitaires et les groupes d'évaluation depuis bientôt une dizaine d'années, leur réponse n'a pas entraîné de remaniement des systèmes complexes de vidéosurveillance actuellement en place. Une « stratégie nationale » a été plutôt proposée pour aborder les insuffisances de l'expansion jusqu'alors « désorganisée et graduelle » de la vidéosurveillance de ces dernières années. Ce ne serait bien sûr pas la première fois que les responsables politiques de la justice pénale demandent de résoudre les carences perçues d'une première solution apparemment insuffisante par une dose de la même solution « en mieux ».

Sans surprise, la British Security Industry Association (Association britannique de l'industrie de la sécurité) n'est pas du même avis. Selon son porte-parole, bien que l'expansion de la vidéosurveillance ait été fragmentaire, les forces de police sont les vraies responsables de ne pas avoir utilisé au maximum le potentiel de ce système. Il semble que, comme pour d'autres domaines de la justice pénale, une troublante « circularité » de la pensée semble prévaloir. Quels que soient les problèmes liés à la vidéosurveillance, il semblerait que la solution réside dans son renforcement et sa multiplication. Notre police et notre industrie de la sécurité semblent être d'accord sur ce point. Toutefois, la véritable problématique, et ceci doit être une leçon pour les autres sociétés, est d'essayer de sortir des sentiers battus, voir même hors du champ des caméras.

Plus récemment, un soutien enthousiaste provenant d'une autre source de police s'est fait entendre pour la vidéosurveillance. Dans ses mémoires controversées, *The Terrorist Hunters* (les chasseurs de terroristes), Andy Hayman, l'ancien commissaire-adjoint de la Police Métropolitaine, a parlé de l'importante contribution des technologies de surveillance au maintien de l'ordre actuel : « Malgré les inquiétudes des groupes de libertés civiles, cette société de surveillance par caméra de vidéosurveillance, utilisant les dispositifs et bases de données d'enregistrement

de nos échanges téléphoniques et par email, les casiers judiciaires et les fichiers d'immatriculation des véhicules et tous les autres dispositifs qui vous viennent à l'esprit, s'avère être efficace pour confondre les délinquants et les terroristes ».

C'est une opinion qui recoupe de nombreuses problématiques au cœur des questions sur le rôle de la vidéosurveillance dans la gestion efficace de la sécurité publique.

En premier lieu, Hayman présente la contribution des technologies de surveillance « malgré les préoccupations des groupes de libertés civiles », comme s'il y avait obligatoirement une contradiction implicite entre le maintien de l'ordre et la liberté. Ce n'est pas nécessairement le cas, bien que ce débat nous ramène au début du maintien de l'ordre par des policiers en uniforme à Londres. Comme le remarquait Robert Peel, fondateur de la Police Métropolitaine en 1829, « la liberté, ce n'est pas d'avoir votre maison cambriolée par des voleurs organisés ou d'abandonner les rues de Londres aux femmes et aux vagabonds éméchés ». Lorsqu'elle est correctement mise en place, convenablement exploitée et efficacement supervisée, la surveillance peut améliorer la sécurité et la liberté.

Pourtant, Hayman mentionne également les technologies de surveillance autre que la vidéosurveillance, appuyant le fait que tout ce domaine de maintien de l'ordre et de gestion de la sécurité a rapidement évolué ces dernières années, à tel point que les implications sociales, les lois et les principes de gouvernance n'ont pas suivi le potentiel technologique. Pourtant, une certaine dérive est possible lorsque les technologies sont utilisées pour des objectifs autres que ceux prévus. Il en résulte des investissements

coûteux et inadéquats et des soi-disant solutions (« solutions technologies ») qui sont inefficaces. Dès lors que le système ne rapporte pas les effets escomptés, cela conduit au scepticisme et à la désillusion.

Certaines de ces difficultés se sont avérées réelles lors de l'utilisation de la vidéosurveillance - par exemple, lors des enquêtes sur les attentats-suicides de 2005 à Londres, par « le manque d'intégration [du système], la qualité des images et les difficultés à récupérer des images numériques ». De plus, au moins une des études a conclu qu'une amélioration de l'éclairage public pouvait avoir un impact plus important sur la prévention de la criminalité enregistrée par vidéosurveillance (Farrington et Welsh, 2002). Et l'éclairage public est nettement moins coûteux.

De manière similaire, Hayman parle de l'utilisation des technologies de surveillance pour « piéger des délinquants et des terroristes » alors que l'adoption généralisée des systèmes de vidéosurveillance des lieux publics au Royaume-Uni était avant tout basée sur le potentiel de prévention de la criminalité. Il était supposé que la vidéosurveillance, exploitée selon le paradigme des mesures de prévention situationnelles, dissuaderaient les délinquants en les rendant visibles et identifiables et en appliquant le principe de « garde » selon la théorie des habitudes de vie à des zones normalement non surveillées.

Les deux approches suggèrent une connexion entre la surveillance et le choix rationnel, que le fait d'être observé et filmé influence le comportement et dissuade la délinquance. Cependant, en pratique, il s'est avéré que la vidéosurveillance avait peu d'impact sur certains types de délit, par exemple pour les

violences interpersonnelles (peut-être dues à l'influence de l'alcool). En fait, la quasi-totalité des programmes d'évaluation mis en place pour surveiller l'efficacité des caméras de vidéosurveillance sur les délits en centre-ville ne sont pas allés plus loin que l'évaluation de l'impact de la vidéosurveillance sur les variations du nombre de crimes enregistrés. Peu d'études sur la vidéosurveillance ont exploré la gestion des incidents, le développement des preuves, la préparation et la poursuite judiciaire de cas, même si les officiers de police se rendaient compte qu'il s'agissait là des principaux avantages de la vidéosurveillance.

Un dernier point sur les observations d'Hayman concerne ce que l'on pourrait appeler « le point de vue de la police ». La police fait souvent partie des plus grands partisans de la vidéosurveillance et lorsqu'on lui présente une nouvelle technologie de contrôle de la criminalité, elle est généralement prête à la tester. Toutefois, la police n'est peut-être pas la mieux équipée pour effectuer une analyse du problème, et pendant longtemps, la vidéosurveillance en Grande-Bretagne était assimilée à un « remède cherchant une maladie ». Les commentateurs avaient la forte intuition que la vidéosurveillance influencerait (ou du moins devrait influencer) le taux de criminalité, mais il y avait peu de preuves de son efficacité.

Certains commentateurs étaient sceptiques, argumentant que les chefs de police adoptaient la vidéosurveillance pour réduire les ressources requises et le nombre de patrouilles de police dans certaines zones. Parfois, le lobbying et le marketing pour la vidéosurveillance par l'industrie de la sécurité ont été remis en question. Ainsi, le marketing par des intérêts particuliers a peut-être généré des attentes irréalistes sur ce que les caméras de vidéosurveillance pouvaient faire.

Face à ces intérêts particuliers, une évaluation indépendante de la vidéosurveillance semble incontournable. Toutefois, les premières évaluations de vidéosurveillance étaient souvent limitées aux simples questions d'impact de la réduction de la délinquance. Le rôle potentiellement plus large que les technologies de vidéosurveillance auraient pu avoir sur un vaste éventail d'activités de maintien de l'ordre a été plutôt négligé : un cas de vision restreinte peut-être. En cas de nouveaux systèmes de vidéosurveillance ou de modernisation et de développement de systèmes existants, ces problématiques devront être prises en compte de façon appropriée – ces systèmes devront peut-être être adaptés pour une variété d'objectifs identifiés par le ministère de l'Intérieur et l'ACPO.

Il existe également de nombreuses plaintes de l'équipe même d'évaluation de la vidéosurveillance ACPO concernant « la grande variabilité de qualité des images enregistrées par les systèmes de vidéosurveillance », alors que d'après des sources non confirmées, « plus de 80 % des images de vidéosurveillance fournies par la police sont loin d'être parfaites, surtout lorsqu'elles sont fournies dans des buts d'identification ».

Enfin le cas de surveillance des citoyens, de responsabilité publique et de surveillance indépendante en ce qui concerne la vidéosurveillance est aussi important que pour les autres méthodes actuelles de maintien de l'ordre. Non seulement c'est important pour que le public comprenne les objectifs de la vidéosurveillance mais aussi les accepte. Ainsi, alors que la confiance du public est renforcée, les systèmes de maintien de l'ordre sont plus efficaces. C'est un domaine souvent ignoré, même dans le récent document de stratégie pour la vidéosurveillance préparé par le ministère de l'Intérieur britannique. Alors que

le document aborde la nécessité d'une collaboration inter agence, l'importance des intervenants et partenaires locaux et le besoin d'une gouvernance et d'un contrôle efficace des programmes de vidéosurveillance, il ne mentionne pas les niveaux de responsabilité locale qui pourraient être appliqués à de tels systèmes de surveillance.

Une référence est faite aux processus nationaux de contrôle et d'inspection tels que le Commissaire à l'Information et le Commissaire à la Surveillance britanniques, mais les dispositions locales sont négligées, même s'il existe de nombreux exemples ou modèles dont s'inspirer. Inversement, ceci peut être un domaine où les différentes cultures politiques ou traditions de maintien de l'ordre proposent des solutions alternatives. Après tout, la question n'est pas d'imposer des solutions « fourre-tout » à des cultures européennes différentes mais plutôt de soulever des questions qui, par expérience, se sont avérées importantes dès que la vidéosurveillance entre en compte. Comme l'affirme Gras, un certain nombre d'autres cultures, notamment en Allemagne, France, Hollande et Suède, pourrait prétendre à des règlementations plutôt plus strictes qu'au Royaume-Uni. Pour sa part, lors de son discours à la conférence de l'Efus à Saragosse, Riches a fait remarqué qu'en Grande-Bretagne, la vidéosurveillance s'est développée de façon largement pragmatique sans vraiment prendre en compte les problèmes de supervision et de contrôle avant que les systèmes soient installés et exploités.

CONCLUSIONS

Analyse des problèmes et mise en œuvre

En rassemblant ces différentes problématiques, d'importantes leçons peuvent être tirées des expé-

riences les plus réussies d'installation et d'exploitation de la vidéosurveillance au Royaume-Uni. En premier lieu, il convient de noter la conclusion quelque peu surprenante de Martin Gill et Angela Spriggs dans leur évaluation de 2005 pour le Ministère de l'Intérieur britannique :

Il serait facile de conclure... que la vidéosurveillance n'est pas efficace : la majorité des programmes évalués n'a pas permis la réduction de la criminalité et même si une réduction a été constatée, elle n'était principalement pas due à la vidéosurveillance. Les programmes de vidéosurveillance n'ont pas non plus rassuré la population et encore moins modifié son comportement.

Avec une telle conclusion, c'est à se demander pourquoi le développement de la vidéosurveillance en Grande-Bretagne a pris une telle ampleur. Outre les questions politiques, nous devons également prendre en compte d'autres questions liées à la mise en œuvre de la vidéosurveillance. En particulier, quels sont les chefs de sécurité et la police qui ont souvent été lents à reconnaître les problèmes et à agir en conséquence. Comme le mentionnent Gill et Spriggs, la suggestion que la vidéosurveillance est un échec est aussi trompeuse que les revendications ambitieuses de l'industrie de la sécurité au regard de la vidéosurveillance.

Pour un avis plus nuancé et basé sur des preuves, nous devons garder à l'esprit un certain nombre de problèmes et envisager un certain nombre de facteurs.

Les taux de criminalité ou les incidents criminels seuls ne sont pas nécessairement un bon indicateur des problèmes criminels et de désordre, ni des craintes et préoccupations du public dans un quartier ou encore de la qualité et de l'expérience de la

sécurité pour une population donnée dans sa communauté. Les initiatives de maintien de l'ordre et prévention de la criminalité doivent tenir compte de cette complexité.

Les rôles et objectifs complexes et variés d'un système de vidéosurveillance sont les suivants : développement du renseignement, collecte de preuves, gestion des incidents et maintien de l'ordre. Tous ces points doivent être reconnus. Les mesures de réduction situationnelle de la criminalité, par prévention ou dissuasion, ne représentent pas le seul résultat attendu. Il est vital que les différents objectifs soient clairs. Comme le remarquait le ministère de l'Intérieur dans son évaluation de 2003 sur la mise en œuvre de projets de vidéosurveillance : « Lors de l'évaluation sur le type de mécanisme de prévention de la criminalité à utiliser, il est important de clarifier les problèmes dans le quartier et de spécifier les capacités du système de vidéosurveillance pour y remédier. Si les deux ne se rejoignent pas, la vidéosurveillance n'est pas la bonne solution ».

Enfin, les systèmes de vidéosurveillance doivent être intégrés à des initiatives existantes de maintien de l'ordre et de gestion de la criminalité. Ceci peut impliquer des modifications de certains autres processus de maintien de l'ordre. Il est assez irréaliste de penser que les systèmes de vidéosurveillance ont, à eux seuls, un impact sur le long terme. De la même façon, les priorités pour le maintien de l'ordre doivent être définies par rapport aux problèmes demandant une solution et non par des suppositions sur le besoin de caméras de vidéosurveillance.

Dès 1999, les recommandations du ministère de l'Intérieur pour les partenariats de développement de la vidéosurveillance soulignaient que toute de-

mande d'investissement devait établir « les critères d'identification du mécanisme de prévention approprié ». Ceci revenait à dire que tout projet de vidéosurveillance devait être étayée par la preuve de « principes de réduction de la criminalité théoriquement solides qui suggèrent des mécanismes de causalité plausibles par lesquels [les système de vidéosurveillance] pourraient avoir un impact sur la criminalité ou les problèmes de désordre dans le contexte actuel ».

Toutefois, Gill et Spriggs ont ensuite déclaré dans leur rapport final que même là où les projets de vidéosurveillance avaient des objectifs discernables qui « devaient être inclus dans les appels d'offres », ces mêmes objectifs « étaient rarement le moteur de ces programmes…et qu'ils étaient rarement intégrés dans la pratique quotidienne ». Ainsi, même si les demandes de financement incluaient des justifications et une analyse des problèmes, ceux-ci étaient souvent négligés après l'obtention des fonds.

Réduction de la criminalité et impacts sur la sécurité de la communauté

Lorsque, dans son rapport sur la stratégie nationale de vidéosurveillance (*National CCTV Strategy*), le ministère de l'Intérieur affirmait en 2007 qu' « il y a un débat en cours sur l'efficacité de la vidéosurveillance pour réduire et prévenir la criminalité », le ministère cherchait de toute évidence, et c'est compréhensible, à poursuivre ce débat. En fait, les preuves accumulées par la recherche et les évaluations, un mélange de résultats mitigés, peu impressionnants, parfois décevants et peu fiables, sont très intéressants.
De nombreuses études locales ont été effectuées au Royaume-Uni à la suite de différentes vagues d'installations de systèmes de vidéosurveillance. Ces

études n'étaient pas toujours très méthodiques ni rigoureuses et souvent limitées à des études d'impact. Nombre d'entre elles étaient également de trop courte durée pour donner des informations fiables sur l'influence sur les tendances criminelles à long terme. Ceci dit, plus récemment, un certain nombre de projets plus importants et/ou de comparaison ont commencé à émerger pour donner une image d'ensemble des évaluations.

En 2002, Brandon Welsh et David Farrington ont entrepris un projet d'évaluation de 46 systèmes de vidéosurveillance dans le monde entier pour le ministère de l'Intérieur.

Les résultats furent mitigés, la moitié des études admissibles « démontrant un impact positif sur la criminalité », alors que cinq démontraient un impact « néfaste » et les cinq dernières, aucun impact. Les programmes de vidéosurveillance en Grande-Bretagne démontrèrent un plus vaste éventail d'impact qu'en Amérique du Nord. De plus, la vidéosurveillance « n'avait eu aucun impact sur les crimes violents mais…un impact désiré sur les délits sur les véhicules et sur les délits dans les parcs de stationnement ». Enfin, « dans le centre-ville et aux alentours des logements sociaux, il semble que la vidéosurveillance ait contribué à une réduction négligeable de la criminalité de 2 % dans les zones expérimentales comparé aux zones de contrôle ».

En remarquant que les « études de surveillance » étaient un domaine relativement nouveau, les auteurs ont suggéré que des recherches supplémentaires étaient nécessaires, autant sur les conditions optimales pour assurer l'efficacité de la vidéosurveillance que sur les mécanismes permettant l'obtention de résultats positifs. Il semblait plutôt clair

qu'un ensemble approprié d'interventions était nécessaire pour obtenir les meilleurs résultats possibles. Ils ont ensuite conclu, de façon plutôt optimiste, que « dans une faible mesure, la vidéosurveillance réduisait la criminalité ». Ils ont recommandé que « les futurs programmes de vidéosurveillance devraient être soigneusement mis en œuvre dans des contextes différents et utiliser des concepts d'évaluation de grande qualité avec un suivi sur le long terme. Au final, une approche de prévention de la criminalité, basée sur les preuves et utilisant les techniques scientifiques les plus poussées, semble donner la formule la plus propice à la construction d'une société plus sûre ».

De telles conclusions sur les impacts de la vidéosurveillance ont été confirmées par de nombreuses autres études similaires, plus particulièrement l'importante étude nationale de Gill et Spriggs en 2005. Ces auteurs ont conclu que la vidéosurveillance semblait avoir un effet limité sur la réduction de la criminalité dans les centres-villes et les zones résidentielles mais semblait mieux marcher dans les endroits plus restreints et d'accès contrôlé (hôpitaux, parkings, centres commerciaux). La vidéosurveillance avait peu d'effet sur la violence et les délits dûs à l'alcool, mais a donné de meilleurs résultats sur les crimes prémédités.

Comme pour les autres études, ils ont également noté un effet de « halo », autrement dit une réduction de la criminalité dans les zones adjacentes et un déplacement des délits. Les caractéristiques techniques de certains systèmes semblent avoir une influence marginale (négative ou positive) sur l'efficacité de ces systèmes. Au final, les sondages auprès du public dans toutes les zones équipées de vidéosurveillance montrent peu d'incidence sur le comportement, les craintes et les préoccupations concernant la criminalité.

Gill et Spriggs concluaient ainsi : « Basé sur les informations présentées dans ce rapport, la vidéosurveillance ne peut pas être considérée comme un succès. Elle a un coût élevé et ne donne pas les résultats anticipés ». Toutefois, ils notent que des leçons sont tirées et que la technologie se modernise rapidement avec des systèmes se basant sur les évènements, proactifs, avec des systèmes « intelligents » biométriques et de reconnaissance du comportement proposant des nouvelles possibilités de gestion de la sécurité, tout en apportant de nouvelles menaces et de nouveaux défis.

Surtout, leur conclusion basée sur une analyse empirique est un avertissement contre toutes les tentations de résoudre les problèmes par des solutions techniques. La vidéosurveillance est seulement un outil. Dans les cas où elle a semblé échouer, les attentes étaient trop importantes ou elle était utilisée dans les mauvais endroits pour les mauvaises raisons. Dans ces cas-là, la vidéosurveillance a peut-être été mal planifiée ou mal mise en œuvre. Elle n'a peut-être pas été efficacement intégrée dans les stratégies de sécurité et les systèmes de maintien de l'ordre de la communauté.

Comme le fait remarquer Kevin Haggarty, un criminologue canadien qui écrit sur le thème de la surveillance, peut-être un des mythes séduisants que nous devons remettre en question est qu'il existe des « solutions de surveillance » à des problèmes sociaux. Ce à quoi le ministère de l'Intérieur a fait allusion en 2007 en déclarant que « la recherche… de la panacée en vidéosurveillance » est probablement futile. De telles « solutions » vont générer sans aucun doute des problèmes et des dilemmes supplémentaires.

Les problématiques peuvent inclure la question de savoir à qui profite la protection de cette surveillance : dans les centres villes britanniques, les zones commerciales riches ont été les premières bénéficiaires, à l'inverse des zones résidentielles, des aires de jeu et des écoles. Ces zones commerciales n'étaient pas nécessairement les communautés prioritaires évidentes ou les zones les plus dans le besoin. Mais la nature des financements des premiers programmes faisait que les occupants de ces zones avaient les moyens de financer les coûts d'investissement correspondants.

Un autre problème d'inégalité se pose : qui sont les personnes filmées par les caméras ? Qui est le plus fréquemment sous surveillance ? Les processus de surveillance soulèvent de profondes questions éthiques et sociales.

Ces questions éthiques élargissent la définition des problèmes de criminalité et de sécurité que nous cherchons à résoudre et ce jusqu'à la conception, la supervision et l'intégration des systèmes développés. Elles impliquent également les processus de contrôle, de supervision, d'évaluation, de responsabilité et de recours nécessaires à une stratégie de sécurité efficace pour la communauté. Si ces questions ne sont pas prises en compte à toutes les étapes, certains problèmes risquent d'apparaître et diminuer l'efficacité même du système. Aussi techniquement sophistiqué que soit le système, ce dernier ne sera qu'aussi efficace que les personnes l'exploitant. Il ne pourra améliorer la sécurité dans la communauté que s'il répond aux besoins des citoyens et les rassure.

Comme l'ont déclaré Gill et Spriggs, il ne faut pas trop attendre de la vidéosurveillance. Ce n'est qu'une solution technique. La vidéosurveillance a besoin de

l'intervention humaine pour être la plus efficace possible parce que les problèmes rencontrés sont complexes. Elle peut réduire la criminalité et renforcer le sentiment de sécurité du public, mais elle peut apporter d'autres avantages. Toutefois, pour bénéficier de ces avantages, il est nécessaire de reconnaître que la réduction et la prévention de la criminalité ne sont pas choses faciles et que des solutions mal conçues ont peu de chance de marcher, quel que soit l'investissement.

REMARQUE : ceci est une version éditée de l'article de Peter Squires. La version complète est disponible en ligne à partir de la page suivante : http://www.brighton.ac.uk/sass/contact/details.php?uid=pas1

Bibliographie

Armitage, R. 2002 *To CCTV or not to CCTV?* London, Nacro.

Brown, B. 1995 *CCTV in Town Centres: Three Case Studies, Crime Prevention and Detection Series,* no.73. London: HMSO. Deane, A. and Sharpe, D. 2009 Big Brother is watching: A comprehensive analysis of the number of CCTV cameras controlled by local authorities in Britain in 2009. London, www.bigbrotherwatch.org.uk

Clarke, R.V. 1995 Situational crime prevention. In M. Tonry and D.P. Farrington (eds.), *Building a Safer Society: Strategic Approaches to Crime Prevention*: Vol. 19. *Crime and Justice: A Review of Research* (pp. 91-150). Chicago, Illinois: University of Chicago Press.

Clarke, R. V. and M. Felson (Eds.) (1993). *Routine Activity and Rational Choice. Advances in Criminological Theory*, Vol 5. New Brunswick, NJ: Transaction Books.

Crawford, A. 1998 Crime Prevention and Community Safety: Politics, Policies and Practices. London, Longman.

Farrington, D.P. and Welsh, B.W. 2002. *Effects of improved street lighting on crime: a systematic approach,* Home Office Research Study 251.

Felson, M. 1998 *Crime and Everyday Life*, Second Edition. Thousand Oaks, CA: Pine Forge Press.

Gras, M.L. 2004 The Legal Regulation of CCTV in Europe. *Surveillance & Society* CCTV Special (eds. C. Norris, M. McCahill and Wood) 2(2/3): 216-229

Garland. D. 2001 *The Culture of Control,* Oxford, Oxford University Press.

Gill M. and Spriggs, A. 2005 *Assessing the Impact of CCTV.* Home Office Research Study No. 292. London: Home Office Development and Statistics Directorate.

Gill M. et al., 2003 *National Evaluation of CCTV: Early Findings on Scheme Implementation – Effective Practice Guide*. Scarman Centre National Evaluation Team, London, Home Office Development and Practice Report No. 7.

Haggarty, K. D. 2009 'Ten thousand times larger' – Anticipating the expansion of surveillance, in B. Goold and D. Neyland (eds) *New Directions in Surveillance and Privacy*. Cullompton, Willan Publishing.
TV Evaluation Team

Hayman, A. 2009 The Terrorist Hunters: The ultimate inside story of Britain's fight against terror, (with M. Gilmore). London, Bantam Press.

Home Office/Association of Chief Police Officers (ACPO) 2007 *National CCTV Strategy. London*, Home Office.
Hope, T. 2001, Crime victimisation and inequality in risk society, in R. Matthews and J. Pitts (ed.) *Crime, Disorder and Community Safety*. London, Routledge

Honess, T. and Charman, E., 1992, *'Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Police Research Group Crime Prevention Unit, 35, London: Home Office Police Department.

ICO (Information Commissioner's Office) 2008 CCTV *Code of Practice: Revised Edition*. ICO Office, Wilmslow: www.ico.gov.uk

Loader, I. 2008 Evidence to the House of Lords Select Committee on the Constitution: *Surveillance, Citizens and the State*. May 14th 2008.

Norris, C., Moran, J., and Armstrong, G., 1998 Surveillance, *Closed Circuit Television and Social Control,* Aldershot: Ashgate.

Norris, C., and Armstrong, G., 1999 *The Maximum Surveillance Society: The Rise of CCTV*. Oxford, Berg Publishers.

Riches, J. 2006 CCTV: Does it work? EFUS: Zaragoza Conference. http://zaragoza2006.fesu.org/IMG/pdf/CCTV_PresentationJames_RICHES.pdf

Shearing, C. 2000 Exclusion From Public Space. in Ethical and Social Perspectives on Situational Crime Prevention. (eds) A. von Hirsch, D. Garland and A. Wakefield. Oxford, Hart Publishing, 2000.
Short, E. and Ditton, J. 1998 «Seen and Now Heard: Talking to the Targets of Open Street CCTV», *British Journal of Criminology*, 38/3: 404-428.

Skinns, D. 1998 «Crime Reduction, Diffusion and Displacement: Evaluating the Effectiveness of CCTV», in C. Norris, J. Moran, and G. Armstrong (eds.): *Surveillance, Closed Circuit Television and Social Control, Aldershot: Ashgate.*

Squires, P. 2006 Introduction: Asking Questions of Community Safety, in Squires, (ed.) *Community Safety: Critical Perspectives on Policy and Practice*. Bristol, The Policy Press.

Squires, P. and Measor, L. (1996a). *CCTV Surveillance and Crime Prevention in Brighton: Half-Yearly Analysis.* Brighton: Health and Social Policy Research Centre, University of Brighton.

Squires, P. and Measor, L. (1996b). *CCTV Surveillance and Crime Prevention in Brighton: Follow-up Analysis.* Brighton: Health and Social Policy Research Centre, University of Brighton.

Surveillance Studies Network, 2007 Evidence to the House of Lords Select Committee on the Constitution: *Surveillance, Citizens and the State*. 28th November 2007.

Von Hirsch, A. 2000 The Ethics of Public Television Surveillance, in Ethical and Social Perspectives on Situational Crime Prevention. (Eds) A. von Hirsch, D. Garland and A. Wakefield. Oxford, Hart Publishing.
Wacquant, L. 2009 Punishing the Poor: The Neo-Liberal Government of Social Insecurity, Duke University Press.

Welsh, B. and Farrington, D. 2002 *Crime Prevention Effects of Closed Circuit Television: A Systematic Review, Home Office Research Study*, No.252, London: HMSO.

« Privacy by design » ou la protection des données personnelles par conception : le cas de la vidéosurveillance

Jeroen van den Hoven
Université de Technologie de Delft (Pays-Bas)

➤ Je défends le principe de protection des données personnelles (méthode « Privacy by design ») dès la conception du système de vidéosurveillance utilisé dans un but de maintien de l'ordre et de sécurité. Ceci permet de surmonter les profondes controverses idéologiques, politiques et philosophiques concernant la nature et l'importance de la protection des données personnelles. La prise en compte de la vie privée dès la conception du système devient rapidement plus importante dans les politiques de protection des données et dans l'ingénierie des systèmes. L'Union européenne (UE) encourage cette idée comme une nouvelle norme dans *Les lignes directrices de la vidéosurveillance du CEDP* (Bruxelles, 17 mars 2010, p.10) :
« La protection des données et de la vie privée devrait être incluse dans les spécifications de conception de la technologie utilisée par les institutions ainsi que dans leurs pratiques.»

Cette approche me semble à privilégier, mais pour que cette idée marche, deux conditions doivent être remplies :
➤1 – nous devons nous rendre compte que les méthodes *Privacy by Design* ou *Privacy Enhancing* (permettant de respecter la vie privée) font partie d'une approche globale d'innovation technique. Cette approche est parfois appelée *Value Sensitive Design* ou *Design for Values* (conception prenant les valeurs

éthiques en considération). Elle demande une méthodologie particulière de façon à éviter les improvisations dans la conception des logiciels qui pourraient favoriser le manque de transparence et de prise de responsabilité.

➤2 - *Privacy by Design* ne peut réussir que si les valeurs morales sous-jacentes à la protection des données personnelles sont claires et si nous recevons une explication détaillée des justifications morales autour de la protection de ces mêmes données. En effet, toutes les décisions, si minimes soient-elles, prises au moment de la conception, devront être justifiées sur la base de considérations morales claires et convaincantes.

La question de la protection de la vie privée est au cœur d'un débat actuel dans la majorité des pays démocratiques entre les libéraux et les communautaristes sur la question de l'équilibre entre les droits individuels, les biens collectifs et les intérêts de la communauté. Dans le cas de la question sur la vie privée, ce débat oppose ceux qui argumentent qu'il est nécessaire de protéger la vie privée des individus en limitant l'accès aux informations personnelles et ceux qui pensent qu'il est nécessaire d'élargir cet accès pour le bénéfice de la communauté. Certains ont fait valoir qu'il s'agissait d'une opposition artificielle, mais une certaine tension demeure qui émerge dans divers cas de violation de la vie privée, par exemple, lors des actions policières secrètes sur internet, de la divulgation de dossiers médicaux pour des raisons d'assurance santé ou pour des recherches épidémiologiques, de l'échange d'informations entre bases de données pour détecter les fraudes à la sécurité sociale, de la demande d'information à des fournisseurs de services internet concernant le comportement en ligne des utilisateurs pour des cas de

justice pénale et lors de l'utilisation de la vidéosurveillance dans les lieux publics pour la prévention de la criminalité.

Le philosophe politique Michael Walzer fait l'observation pertinente que « le libéralisme est rongé par les problèmes dus aux profiteurs, ces personnes qui continuent à bénéficier des avantages d'une appartenance et d'une identité tout en ne participant plus aux activités qui permettent d'obtenir ces mêmes avantages. En revanche, le communautarisme est le rêve d'une société sans profiteurs ».[1] Les communautaristes considèrent ces techniques d'information comme des moyens d'attendre cette société sans profiteurs.

La vie privée a également été le sujet de nombreuses discussions philosophiques (Nissenbaum, 2004; Roessler 2005; Decew, 1997, Van den Hoven 2009) et de nombreux auteurs différents ont présenté leurs visions de la définition de la vie privée. Différentes explications conceptuelles et philosophies proposent des réponses différentes à la question de savoir ce que signifie la vie privée et en quoi elle est importante. Malheureusement, il n'y a guère de consensus et sans doute n'y en aura-t-il pas davantage à l'avenir.

Le concept actuel que la vie privée est complètement obsolète s'ajoute à la controverse, « vous n'avez aucun anonymat, passez à autre chose ». A cause des technologies modernes, la vie privée est devenue une chose du passé, nous devrions l'accepter.

De nombreux concepts servent de base à l'idée de vie privée. Sa signification exacte n'est pas vraiment comprise et la façon dont la technologie, le génie logiciel et le développement des systèmes l'affectent non plus. Pour des raisons pratiques, telles que la

formulation et la préparation des lois ainsi que les politiques et les technologies, les malentendus de conception et la confusion sur la nature et l'importance de la vie privée conduisent à une indécision pratique, des délais, de l'inefficacité, des coûts élevés et des échecs lors des projets TIC.

Il est nécessaire aujourd'hui de « reconstruire » la notion de vie privée pour progresser et régler les problèmes urgents auxquels nous faisons face jour après jour, sans s'enliser dans d'interminables débats.

Le rôle principal donné au concept de *vie privée* lorsque nous débattons des questions morales autour de la protection des données personnelles obscurcit la recherche de solutions pratiques. Nous restons alors bloqués dans une profonde controverse sans solution sur la nature du Soi et de la Communauté, opposant les libéraux et les communautaristes. Comme il n'est pas facile de prendre parti, je suggère que nous abordions le problème d'un autre point de vue en se posant simplement la question suivante : Pourquoi devrions-nous protéger les données personnelles ? Quelles sont les raisons morales qui nous poussent à le faire ? Pouvons-nous penser que nous devrions les protéger comme nous protégeons, disons, les réacteurs nucléaires, les manuscrits médiévaux, les bébés ou les sanctuaires d'oiseaux ? Dans chacun de ces cas, nous avons de bonnes raisons de restreindre l'accès, de limiter les heures de visite, de stipuler les comportements appropriés, les personnes qui sont autorisées à s'approcher et de quelle manière. Dans chaque exemple, la protection prend une forme différente et a une logique différente. Quelle serait une bonne raison morale de protéger les données personnelles et quel type de raison pourrait justifier de limiter le droit d'accès des autres à ces données ?

Les raisons morales pour lesquelles nous devrions être inquiets pour nos données personnelles sont les mêmes raisons qui justifient que nous limitions l'accès à nos données et leur utilisation par des tiers. Les raisons sont les suivantes :

Tout d'abord, la protection des individus dont les données personnelles sont disponibles au public. Dans une société d'information, les personnes courent le risque d'être blessées quand et parce que leurs données personnelles sont accessibles. Nous souhaiterions éviter l'utilisation des données personnelles contre les personnes concernées.

La seconde raison concerne l'équité sur le marché des données personnelles. Nous protégeons les données personnelles et avons des lois à cet effet, parce que de nombreuses personnes souhaiteraient y avoir un accès facile et peu coûteux. De nombreuses personnes et organismes ont de bonnes raisons de cacher au public la valeur marchande des données personnelles ainsi que l'utilisation qui peut en être faite. Les contrats proposés aux clients pour accéder à leurs données personnelles, comme les cartes de fidélité, sont souvent injustes. Les régimes de protection des données devraient garantir des accords équitables et protéger les citoyens contre les abus et les entorses aux contrats.

La troisième raison se rapporte à une utilisation juste de l'information. Les données individuelles ont, pour ainsi dire, un « habitat naturel ». Les informations sont rassemblées et échangées dans des situations bien définies et gérées par des groupes bien spécifiques, tels que les docteurs, les officiers de police, les responsables de ressources humaines, les avocats, etc. Il n'est pas approprié de communiquer cette information d'un domaine social à un autre, par

exemple si l'information passe de la sphère médicale à la sphère commerciale ou encore de la sphère familiale à la sphère politique. Ces sphères doivent rester séparées les unes des autres.

Enfin, la dernière raison est que chaque individu a le droit à son autonomie morale et au contrôle de la façon dont il se présente. Les gens veulent être identifiés comme les personnes avec lesquels ils s'identifient aussi. Ils veulent être vus comme la personne qu'ils pensent être. Ceci demande discrétion et un certain choix concernant les informations personnelles qu'ils révèlent. Ceci exige également la protection des données et le respect de la souveraineté de chaque individu sur ses informations personnelles.

Value Sensitive Design et Privacy by Design (conception prenant les valeurs d'éthiques en considération)

L'intégration de la sécurité et la vie privée dans les conceptions, en architecture ou en ingénierie n'est pas une idée nouvelle. Aussi loin que le 18ème siècle, le philosophe Jeremy Bentham a conçu ce qu'il pensait être l'architecture idéale pour les prisons. « La morale réformée, la santé préservée, l'industrie revigorée, l'instruction diffusée, les charges publiques allégées, l'économie fortifiée - le Nœud Gordien des lois sur les pauvres non tranché mais dénoué - tout cela par une simple idée architecturale ! ». Son idée était que la sécurité et le contrôle des prisonniers seraient grandement améliorés par le concept d'une prison en forme de dôme, qu'il appela le « Panoptique ». Ainsi, le balcon d'observation des gardes était situé au centre, leur permettant de voir les prisonniers tout autour d'eux. Ce fût un des premiers exemples d'intégration de concepts dans une conception. De nos jours, l'incorporation de valeurs éthiques

dans la conception d'une technologie quelconque est appelée conception éthique (Value Sensitive Design ou VSD). Privacy by Design est l'une des applications du Value Sensitive Design (conception éthique).

La conception éthique (Value Sensitive Design) intègre les valeurs morales dans la conception d'objets et de systèmes techniques en considérant la conception d'un point de vue éthique et par des recherches sur la façon dont les valeurs morales (par exemple la liberté, l'égalité, la confiance, l'autonomie, la vie privée ou la justice) peuvent être favorisées ou freinées par la conception même (Friedman 1997; Friedman 2005). La conception éthique (Value Sensitive Design) se concentre *essentiellement et spécifiquement* sur les valeurs *morales*, alors que la conception traditionnelle se concentre plutôt sur les exigences de fonctionnement, telles que la vitesse, l'efficacité, la capacité de stockage ou la facilité d'utilisation. Bien que la construction d'une technologie conviviale puisse avoir l'effet secondaire d'accroître la confiance ou la sensation d'autonomie de l'utilisateur, lors de la conception éthique (Value Sensitive Design), l'intégration de valeurs morales dans la conception est un objectif principal plutôt qu'un sous-produit. La conception éthique (Value Sensitive Design) est également « une façon de travailler éthiquement qui a pour but d'intégrer les valeurs morales à la conception, à la recherche et au développement technologiques », comme je l'ai déjà argumenté (Van den Hoven 2005: 4).

La conception éthique (VSD) peut uniquement être utilisée dans le domaine de la protection des données si nous arrivons à décrire clairement les valeurs morales qui doivent être intégrées lors de la conception du système et la façon dont elles peuvent être traduites en « exigences non opérationnelles ».

L'étape suivante est de détailler ces exigences en un ensemble de fonctions extrêmement claires et précises à assigner au système. Mais cette méthodologie n'existe pas encore et le danger est qu'avec l'évolution de la technologie, les systèmes deviennent encore plus opaques qu'ils ne le sont déjà.

La conception éthique (VSD) vise à concilier des valeurs différentes et en opposition dans la conception d'ingénierie ou en cas d'innovation (Van den Hoven 2008b). Ceci est directement applicable aux valeurs opposées en jeu dans le débat sur la vidéosurveillance : la sécurité et la vie privée.

Dans notre société, nous attachons de l'importance à la vie privée, mais, parallèlement, la sécurité et la disponibilité des informations sur les citoyens ont leur importance. Cette tension est illustrée dans les débats sur la vidéosurveillance des lieux publics. Soit nous acceptons d'échanger notre vie privée pour la sécurité en installant des caméras partout, soit nous refusons de le faire au nom du respect de la vie privée, et de ce fait, acceptons une sécurité moindre. Les systèmes de vidéosurveillance intelligents nous permettent d'avoir le beurre et l'argent du beurre. En effet, leur architecture intelligente inclut la fonction de surveillance avec des systèmes qui limitent le débit et la disponibilité des informations enregistrées.

La première génération de caméras de vidéosurveillance offre relativement peu de sécurité. Les images sont floues et elles violent la vie privée des passants en enregistrant leurs déplacements. La deuxième génération propose une bien meilleure qualité et, ainsi, offre plus de sécurité. Mais, c'est justement parce que la qualité des images est si bonne qu'elles sont plus invasives. Maintenant, la troisième génération de « systèmes à caméras intelligentes » enregistre uniquement les évènements suspects et sont équipés d'une fonction intégrée qui bloque l'enregistrement d'images à l'intérieur de maisons privées. C'est là une solution technologique parfaite pour notre dilemme moral. Par exemple, la police de Rotterdam utilise déjà ces systèmes intelligents, équipés de logiciels qui interdisent aux exploitants de filmer à l'intérieur de maisons privées.
Les paramètres technologiques de ces systèmes intelligents peuvent être configurés de manière extrêmement fine de façon à offrir tous les avantages et les fonctions d'une vidéosurveillance avant-garde sans aucune violation des normes de protection des données personnelles. Là où les systèmes précédents étaient basés sur le « tout ou rien », nous avons maintenant une technologie qui nous permet de choisir qui a accès aux enregistrements, dans quelles conditions les images sont stockées et la façon dont les enregistrements peuvent être utilisés et incorporés à d'autres bases de données.

Un trait commun de nombreuses technologies « intelligentes » et innovantes est qu'elles permettent de combiner des valeurs ou des préférences qui étaient auparavant irréconciliables. Par exemple, les technologies environnementales intelligentes permettent d'associer la croissance économique et le développement durable. Les bombes soi-disant « intelligentes » permettent de toucher l'ennemi sans faire de victimes civiles.

Protection des données personnelles par conception : une innovation morale

Il semble légitime d'affirmer que, puisque la société a l'obligation morale de garantir la vie privée de ses citoyens tout en assurant la sécurité dans tous les lieux publics, elle a également l'obligation morale de faire le nécessaire pour satisfaire ces deux obligations. Nous

sommes moralement tenus de continuer les recherches et les innovations sur le modèle de Privacy by Design, une technologie qui permet d'associer sécurité et vie privée.

Une telle entreprise demande un réglage précis de la technologie et une réflexion fine sur la justification morale de la protection des données. De plus, elle demande une méthodologie systémique afin de relier les deux domaines, la technologie et nos valeurs morales.

Bibliographie

Batya Friedman e.a. Value Sensitive Design: Theories and Methods. Technical Reports, Department of Computer Science and Engineering, University of Washington, 2002. Report 02-12-01. http://www.urbanism.org/papers/vsd-theory-methods-tr.pdf

Jeroen Van den Hoven & John Weckert, Information Technology and Moral Philosophy. Cambridge University Press, 2009.

Vidéosurveillance urbaine en Europe : un choix politique ?

Eric Töpfer, université technique de Berlin (Allemagne)

La vidéosurveillance urbaine est devenue un enjeu européen pour la première fois en 1997, lorsqu'elle a été choisie comme l'un des thèmes clés de la conférence européenne sur la « Prévention de la Criminalité » organisée par la présidence hollandaise de l'Union européenne à Noordwijk (Pays-Bas). Il a été conclu lors de la déclaration de clôture de la conférence que :

« Les caméras comme outils de prévention de la criminalité sont, en général, de nouvelles méthodes économiques utilisées pour rassurer les citoyens préoccupés par leur sécurité. Elles servent de dissuasion à la criminalité et peuvent être utilisées pour soutenir une action judiciaire. [Toutefois], les techniques de vidéosurveillance devraient uniquement être utilisées [dans le cadre] d'une politique globale locale et/ou nationale de prévention du crime [...]. De plus elles devraient être supervisées par un personnel qualifié [...]. Le public doit être informé de l'utilisation de la vidéosurveillance. La vie privée doit être protégée. » [1]

C'était alors les débuts de la vidéosurveillance. Trois ans auparavant, en 1994, le ministère de l'Intérieur britannique avait lancé une « révolution de la vidéosurveillance » en finançant une série de compétitions « City Challenge Competitions » avec une première

[1] Recommandations de la conférence européenne "Prévention de la criminalité" 11–14 Mai 1997. Paru dans : European Journal on Criminal Policy and Research, Vol. 5, No. 3 (Septembre 1997), pp. 65-70 (66).

phase de financement se montant à deux millions de livres sterling.[2] En France, en 1995, le parlement votait la Loi Pasqua qui autorisait explicitement le déploiement de la vidéosurveillance dans certains « points chauds » des principales villes françaises. Cette décision avait fait suite à l'installation controversée, deux ans auparavant, de 96 caméras de vidéosurveillance en banlieue parisienne à Levallois-Perret :[3] En République tchèque, le gouvernement commença à financer les initiatives locales de prévention de la criminalité en 1996. Celles-ci incluaient, entre autres, l'installation de systèmes de vidéosurveillance. La même année, en suivant l'exemple tchèque, la police municipale de Leipzig installa une caméra en centre ville, la toute première en Allemagne.[4] En Hollande, le premier système fut installé en 1998, un an seulement après la conférence de Prévention du Crime à Noordwijk. La municipalité d'Ede décida d'installer 12 caméras pour surveiller une zone proche de la gare ferroviaire la nuit. [5]

Fin 1998, en se rapportant à la conférence de Noordwijk, la délégation française lança un débat sur la vidéosurveillance par le groupe de travail « Police Cooperation Working Party » (PCWP) du Conseil de l'Europe. Le rapport du PCWP conclut que « les autorités locales utilisent peu les systèmes de vidéosurveillance, excepté en Grande-Bretagne et en Finlande » et déclara que le PCWP « pourrait promouvoir le développement de tels systèmes ». [6]

Vers l'omniprésence ?

La vidéosurveillance ou la « télévision industrielle » comme on l'appelait à ses débuts, est aussi ancienne que la télévision hertzienne. Toutefois, pendant plusieurs dizaines d'années, l'utilisation des caméras

de surveillance pour le maintien de l'ordre était limitée à la supervision et à la gestion de la circulation ou, occasionnellement, à la surveillance des foules lors d'évènements importants ainsi que pour certaines enquêtes criminelles. La surveillance continue des lieux publics urbains restait une exception. Au Royaume-Uni par exemple, la vidéosurveillance avait seulement été installée dans quelques zones d'intérêt national comme Westminster et Whitehall, où un réseau de caméras avait été installé par la Police Métropolitaine de Londres à la suite des troubles politiques de la fin des années 60.[7]

De nos jours, 13 ans après la conférence hollandaise de prévention de la criminalité, qui visiblement avait lancé le processus de transfert international des politiques, les systèmes de vidéosurveillance ont été installés par milliers dans les villes européennes. Comme l'a prédit, en 1999, Steve Graham, profes-

[2] Norris, C. et al. (2004): The growth of CCTV. A global perspective on the international diffusion of video surveillance in publicly accessible space. Paru dans : *Surveillance & Society,* Vol. 2, No. 2/3, pp. 110-135 (111).

[3] Töpfer, E. & Helten, F. (2005): Marianne und ihre Großen Brüder. Videoüberwachung à la Française. Paru dans : *Bürgerrechte & Polizei/ CILIP*, No. 81, pp. 48-55.

[4] Müller, R. (1997): Pilotprojekt zur Videoüberwachung von Kriminalitätsschwerpunkten in der Leipziger Innenstadt. Paru dans : *Die Polizei*, Vol. 88, No. 3, pp. 77-82.

[5] Gemeente Ede (2000): *Ogen in de nacht. Eindevaluatie cameratoezicht Ede*. Août 2000. En ligne : http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/bestuurlijk-handhaven/cameratoezicht/1_ede_effectevaluatiex2000.pdf.

[6] Conseil de l'Europe : Doc. 5045/99, 12 janvier 1999.

[7] Williams, C. (2003): Police surveillance and the emergence of CCTV in the 1960s. Paru dans : *CCTV,* ed. by M. Gill, Leicester: Perpetuity Press, pp. 9-22.

seur de Géographie Humaine à l'Université de Durham (UK) et un des spécialistes mondiaux du phénomène des cybercités, il semble que la vidéosurveillance soit devenue le cinquième service public de la vie moderne, après l'eau, le gaz, l'électricité et les télécoms.[8]

La montée de la vidéosurveillance « open-street », c'est-à-dire la surveillance de zones urbaines publiques 24h/24 et 7j/7 avec des objectifs fixés de contrôle de la criminalité et de gestion de l'ordre public, a commencé dans les années 80. Trois principaux facteurs expliquent le « boom » de la vidéosurveillance dans les villes européennes :

➤ l'émergence d'un nouveau paradigme sous-jacent des politiques de justice pénale, selon laquelle l'approche traditionnelle qui considérait le crime comme une déviance individuelle a été remplacée par l'idée que le crime émerge de certains groupes ou endroits particuliers considérés comme « criminogènes ». Et ainsi, que le risque puisse être évalué, évité et géré grâce à des méthodes actuarielles.

➤ Le déclin de l'industrie à la base des économies urbaines et la montée du consumérisme et des services, associés à l'émergence du « marketing territorial » ou « marketing urbain ». De nos jours, la sécurité est considérée comme un des éléments clés de l'attrait d'une ville, dans la course mondiale aux investissements et à l'activité économique.

➤ La tendance à la décentralisation qui a vu le contrôle de la criminalité et de l'ordre public pris en charge par les municipalités. De nombreux pays ont accordé aux municipalités l'autorisation juridique explicite d'installer des caméras sur leurs territoires pour lutter contre la criminalité. [9]

La diversité de la vidéosurveillance des lieux publics en Europe

Mis à part les facteurs généraux mentionnés plus haut, il est également important de prendre en compte les spécificités de chaque pays européen ainsi que leurs différents contextes socio-économiques, systèmes institutionnels et expériences en criminalité. Comme le fait remarquer le sociologue canadien David Lyon :

« Il est vrai que certaines similitudes structurelles et problèmes communs auxquels font face les Etats modernes peuvent résulter en des techniques similaires pour des endroits différents. [...] Il est également vrai que selon les contextes locaux, régionaux, sociaux, politiques et culturels, l'expérience de la surveillance sera différente. [...] La simple existence des nouvelles technologies est loin d'être une raison suffisante pour les utiliser. » [10]

Dans le Grand Duché du Luxembourg, le premier système de vidéosurveillance dans la rue a été installé en 2007, 13 ans après que la Grande-Bretagne ait lancé ses compétitions « City Challenge ». [11] En Norvège, un seul système a été installé en 1999 : six caméras exploitées par la police locale d'Oslo. [12]

---

[8] Graham, S. (1999): Towards the fifth utility? On the extension and normalisation of CCTV. Paru dans : *Surveillance, Closed Circuit Television and Social Control*, ed. by C. Norris et al. Aldershot: Ashgate, pp. 89-112.

[9] Pour une argumentation théorique détaillée, voir McCahill, M. (1998): Beyond Foucault. Towards a contemporary theory of surveillance. Paru dans : *Surveillance, Closed Circuit Television and social control,* ed. by C. Norris et al., Aldershot: Ashgate, pp. 41-65.

[10] Lyon, D. (2004): Globalizing surveillance. Comparative and sociological perspectives. Paru dans : *International Sociology*, Vol. 19, No. 2, pp. 135-149 (141-142).

[11] *Tageblatt. Zeitung für Luxemburg*, 12 décembre 2007.

En revanche, le Royaume-Uni est équipé, selon les estimations, de 40 à 50.000 caméras dans les lieux publics dans plus de 500 villes.[13] En France, il est supposé qu'environ 500 municipalités (en général de grosses agglomérations) exploitent approximativement 20.000 caméras. De plus, le ministre de l'Intérieur français a annoncé en 2009 que le nombre de caméras exploitées sur le territoire français serait triplé.[14] En Hollande, un cinquième des 443 autorités locales utilisent la vidéosurveillance dans les lieux publics, soit un total de 4 000 caméras.[15]

En Europe de l'Est, la Pologne, la République tchèque, la Hongrie et les pays baltes sont reconnus pour exploiter des centaines de caméras dans leurs principales villes. Les pays d'Europe du Sud ont des positions variables concernant la vidéosurveillance. Le Portugal et l'Espagne ont été réticents à l'utiliser. La Grèce a installé environ 1200 caméras pour les Jeux Olympiques de 2004, une initiative qui a généré de nombreuses protestations dans la population. Environ 200 caméras ont cependant été conservées à la fin des Jeux.[16] En revanche, des centaines de villes italiennes (communi) utilisent des systèmes de vidéosurveillance.

En Allemagne, où la Conférence des ministres de l'Intérieur de 2000 a approuvé la vidéosurveillance comme « un outil approprié pour soutenir le travail de la police », il y a aujourd'hui moins de 200 caméras en exploitation dans 30 ou 40 villes.[17] En Autriche, où le premier système a été installé en 1994 autour de la gare de Villach, une initiative fédérale a permis une croissance rapide des utilisations de la vidéosurveillance. Après une modification de la loi de Police sur la Sécurité, le ministère de l'Intérieur a annoncé une expansion de la surveillance des lieux publics.

En 2006, cinq villes autrichiennes ont installé des systèmes de vidéosurveillance dans 11 lieux publics. Des demandes ont également été enregistrées pour l'installation de vidéosurveillance dans 17 nouveaux lieux. [18] Au Danemark, le gouvernement a présenté une nouvelle série de mesures destinées à renforcer la sécurité, ce qui inclut, pour la toute première fois, l'autorisation officielle pour la vidéosurveillance dans les lieux publics. [19]

Cette vue d'ensemble montre que l'utilisation de la vidéosurveillance varie de pays à pays. Elle varie également au sein des villes, où certaines zones sont couvertes par un réseau de centaines de caméras, alors que d'autres zones urbaines sont seulement couvertes par de petits systèmes de moins d'une dizaine de caméras.

---

[12] Winge, S. & Knutsson, J. (2003): An evaluation of the CCTV scheme at Oslo Central Railway Station. Paru dans : CCTV, ed. by M. Gill, Leicester: Perpetuity Press, pp. 127-140.

[13] Williams, K. S. & Johnstone, C. (2000): The politics of the selective gaze. Closed Circuit Television and the policing of public space. Paru dans : *Crime, Law and Social Change*, Vol. 34, No. 2, pp. 183-210.

[14] *France Soir*, 16 février 2009.

[15] Dekkers, S. et al. (2007): *Evaluatie Cameratoezicht op Openbare Plaatsen. Éénmeting*. Eindrapport. Regioplan publicatienr. 1515. Amsterdam, Mai 2007, p.IV.

[16] Samatas, M. (2007): Security and surveillance in the Athens 2004 Olympics. Some lessons from a troubled story. In: *International Criminal Justice Review*, Vol. 17, No. 3, pp. 220-238.

[17] Chiffres mis à jour par Töpfer, E. (2005): Polizeiliche Videoüberwachung des öffentlichen Raums. Entwicklung und Perspektiven. In: *Datenschutz Nachrichten*, Vol. 28, No. 2, pp. 5-9.

[18] *Salzburger Nachrichten*, 4 février 2006.

[19] *heise online*, 4 novembre 2005

Soutien et règlementation

Comme le montre régulièrement les sondages, la vidéosurveillance est largement soutenue par les principaux partis politiques ainsi que par le public. Toutefois, le soutien varie suivant l'endroit et l'étendue de la surveillance. Selon un sondage effectué en 2003 dans cinq capitales européennes, 90 % des personnes interrogées à Londres étaient favorables à la vidéosurveillance dans la rue, alors qu'à Vienne, seulement 25 % partageaient cette opinion.[20] En Grande-Bretagne, à la suite du cas Bulger en 1993, il y a eu un large consensus autour de l'idée que la vidéosurveillance pourrait être la « solution miracle » contre la criminalité. Ainsi, des images ont montré deux garçons de 10 ans dans un centre commercial, kidnappant un très jeune enfant de deux ans, James Bulger, dont le corps mutilé avait été retrouvé deux jours plus tard près d'une voie de chemin de fer. Ces images avaient été diffusées pendant plusieurs semaines sur toutes les principales chaines de télévision. Ce cas avait choqué la nation entière, mais promettait une solution « technique » qui empêcherait des évènements aussi terribles de se reproduire.[21]

Toutefois, la vidéosurveillance du type britannique est considérée dans certains pays européens comme une surveillance à la Big Brother. En Allemagne, par exemple, l'ancien ministre fédéral de l'Intérieur, Otto Schily, a soutenu la vidéosurveillance des rues lorsque celle-ci est devenue un enjeu politique à la fin des années 90, mais il a aussi mis en garde le public contre la « surveillance extensive », argumentant qu'elle constituait une violation disproportionnée des droits fondamentaux.[22]

Dans une certaine mesure, de telles opinions reflètent la règlementation juridique de la vidéosurveillance. En Grande-Bretagne, l'expansion du début a eu lieu dans un vide règlementaire : la loi sur l'Informatique et les Libertés de 1984 ne s'applique qu'au traitement des données numériques, ignorant donc les systèmes analogiques mis en place dans les premiers temps. En outre, la législation sur la Justice Pénale et l'Ordre Public de 1994 autorisait de façon explicite les autorités locales à fournir des « équipements d'enregistrement des images lors d'événements dans leur circonscription » et les a exemptées du paiement des licences coûteuses pour le câblage du système, prévues en vertu de la Loi sur les Télécoms. Le cadre règlementaire a seulement changé avec la mise en place de la directive européenne de Protection des Données, grâce à la modernisation de la loi sur l'Informatique et les Libertés de 1998 et à l'intégration, en 2000, de la Convention européenne des Droits de l'Homme dans la loi nationale sur les Droits de l'Homme.

Contrairement à la Grande-Bretagne, la plupart des pays européens ont considéré dès le début de la vidéosurveillance que celle-ci constituait une violation des droits fondamentaux. En 1990, en France, un tribunal administratif de Marseille s'est prononcé contre les plans d'installation d'un réseau de 93 caméras prévus par la mairie d'Avignon, considérant que l'enregistrement optionnel constituait une violation disproportionnée de la vie privée. La vidéosurveillance et l'enregistrement des images n'ont été autorisés qu'en 1995, par la Loi Pasqua, qui a re-

[20] Hempel, L. & Töpfer, E. (2004): *CCTV in Europe. Final report of the Urbaneye Project. Zentrum Technik und Gesellschaft,* TU Berlin. (Urbaneye Working Paper No. 15), p. 44. En ligne : http://www.urbaneye.net/results/ue_wp15.pdf.

[21] McGrath, J. (2004): *Loving Big Brother. Surveillance culture and performance space*, London: Routledge.

[22] Discours au Parlement Fédéral, 9 novembre 2000. Plenarprotokoll 14/130.

commandé son utilisation dans les zones à « forts risques d'agression ou de vol ». [23]

En Allemagne, la décision de « recensement » de 1983 de la Cour constitutionnelle fédérale a développé le concept de « droit à l'autodétermination informationnelle », déclarant que toute collecte de données personnelles sans un consentement éclairé était illégale, sauf dans le cas où elle était entreprise « pour l'intérêt général », conformément au principe de proportionnalité et sur une base juridique claire. Ainsi, la vidéosurveillance en Allemagne est en général contrôlée par la police régionale et limitée aux soi-disant « points chauds ». Une approche juridique similaire qui limite l'utilisation des caméras de vidéosurveillance à des zones plus ou moins clairement définies est également utilisée dans de nombreux autres pays. Toutefois, dans les pays tels que la Hongrie ou la Norvège, la règlementation sur la protection des données est le point de référence juridique. Ceci est également le cas aujourd'hui en Grande-Bretagne. Certaines de ces lois sur l'Informatique et les Libertés mentionnent la vidéosurveillance de façon explicite, alors que d'autres ne la mentionnent qu'en termes généraux. En Grande-Bretagne par exemple, le premier « code de bonnes pratiques de la vidéosurveillance » a été publié en 2000 par le Commissaire à l'Information.[24]

Organisation et supervision

L'organisation de la vidéosurveillance dans les pays européens varie suivant le cadre juridique. Dans certains pays, la surveillance des rues est exclusivement du domaine de la police, qui détient, répare et exploite les systèmes de vidéosurveillance. C'est le cas en Allemagne, où les forces de police régionales des Länder en ont la principale responsabilité, bien

qu'elles partagent parfois des informations avec la police fédérale et les services locaux de maintien de l'ordre public. En Autriche, la police fédérale est en charge de la vidéosurveillance. En Norvège, le système de vidéosurveillance d'Oslo est exploité par la police nationale. Dans d'autres pays, la vidéosurveillance reste sous la responsabilité des autorités locales. En Grande-Bretagne par exemple, il est estimé qu'environ 80 % des systèmes de vidéosurveillance dans les rues appartiennent aux autorités locales qui les exploitent.[25]

Ces systèmes sont en général exploités par les forces de police municipales ou locales (dans les pays où cette dernière existe). La plupart du temps, la gestion réelle de la vidéosurveillance est effectuée par du personnel civil, en collaboration avec les forces de police municipale, régionale et/ou nationale.

Il existe également des exemples de partenariats public-privé. Par exemple, à Vilnius, capitale de la Lituanie, une société de sécurité privée est sous contrat pour le fonctionnement de la salle de contrôle.[26] Au Royaume-Uni, les premiers systèmes de vidéosurveillance ont souvent été cofinancés par les entreprises locales et, dans de nombreux cas, une relation étroite se constituait entre la salle de contrôle de vi-

[23] Section 10 de LOI no 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

[24] Une version mise à jour est disponible sur : http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf.

[25] *CCTV Image*, No. 25 (février 2008), pp. 5-6.

[26] Töpfer, E. (2008): Videoüberwachung in Europa. Entwicklung, Perspektiven und Probleme. Paru dans : *Informatik und Gesellschaft. Verflechtungen und Perspektiven*, ed. by H.-J. Kreowski, Münster: LIT Verlag, pp. 61-82 (65-66).

déosurveillance publique et les programmes privés de surveillance dans les commerces.[27] D'autres initiatives ont été tentées en Grande-Bretagne visant à recruter le public. Par exemple, une expérience a été tentée il y a quelques années à Londres dans le quartier de Shoreditch où les résidents recevaient des images de vidéosurveillance directement sur leur téléviseur. [28]

Une partie de cette diversité en termes d'organisation est due aux régimes de supervision et d'accréditation de chaque pays. Dans de nombreux pays, la vidéosurveillance dans la rue est supervisée par les autorités de protection des données qui sont généralement autorisées à inspecter les systèmes de vidéosurveillance, dénoncer les mauvaises pratiques et recommander les améliorations à apporter à la gestion des données. Toutefois, certains pays n'incluent pas la vidéosurveillance aux sujets sous la tutelle des autorités de protection des données. Ceci est le cas en Autriche. Par exemple, le Représentant de la Protection Juridique (Rechtsschutzbeauftragter) au ministère fédéral de l'Intérieur a l'autorité pour vérifier les systèmes de vidéosurveillance, mais ses recommandations ne sont pas obligatoires. En France, la Commission nationale Informatique et Libertés (CNIL) a été écartée par la « Loi Pasqua » qui a créé une nouvelle instance, la Commission départementale de vidéosurveillance (CDV). Présidée par un juge, celle-ci examine chaque projet de vidéosurveillance et ses membres votent en faveur ou contre le projet. Toutefois, la décision finale revient au Préfet qui est le représentant du gouvernement au niveau du département. La plupart du temps, le Préfet suit les recommandations de la Commission.

Approche globale et approche locale

Le coût est le facteur clé dans la détermination de l'étendue de la vidéosurveillance. Sans surprise, l'expansion de la vidéosurveillance est plus limitée dans les pays où seuls les officiers de police formés sont autorisés à superviser les images de vidéosurveillance dans la salle de contrôle comparée aux pays qui emploient du personnel civil peu payé.
Dans certains pays, le gouvernement central a fait d'importants investissements pour la surveillance des rues. Ceci est le cas au Royaume-Uni, où le ministère de l'Intérieur a financé, entre 1994 et 1998, quatre Compétitions « City Challenge » à hauteur de 85 millions de livres, soit 75 % du budget total de prévention du crime. Le New Labour a suivi la même politique et investi 170 millions de livres dans la CCTV Initiative entre 2002 et 2010.[29]

En République tchèque, un des pays où l'investissement public a été très important, le budget gouvernemental pour la prévention du crime inclut une importante allocation pour la vidéosurveillance. Il en est de même en Italie et en Allemagne où les autorités régionales ont soutenu la vidéosurveillance.

Les gouvernements nationaux et/ou régionaux d'Europe ont encouragé l'adoption locale de la vidéosurveillance, par la mise en place de règles juridiques ainsi que par la provision de ressources financières, mais aussi par la définition des méthodes d'utilisa-

[27] Coleman, R. (2004): *Reclaiming the streets. Surveillance, social control and the city*, Cullompton: Willan Publishing.

[28] *Guardian*, 11 janvier 2006.

[29] Töpfer, Eric (2007): Entgrenzte Raumkontrolle? Videoüberwachung im Neoliberalismus. Paru dans : *Kontrollierte Urbanität. Zur Neoliberalisierung städtischer Sicherheitspolitik*, ed. by V. Eick et al., Bielefeld: transcript, pp. 193-226 (204-206)r 2006.

tion. Dans de nombreux pays, le gouvernement central a publié des lignes directrices pour les autorités locales de façon à éviter une constante réinvention de la roue au niveau local. Le livret du ministère de l'Intérieur britannique *CCTV: Looking Out For You* (Vidéosurveillance : votre protection) publié en 1994, en est un des premiers exemples, bien qu'il ait surtout été utilisé comme outil de promotion plutôt que d'orientation. Le guide *Handreiking Cameratoezicht* publié par le gouvernement hollandais en 2000 est plus détaillé et a été distribué dans toutes les municipalités du pays. Ce guide présente un résumé des expériences de vidéosurveillance des lieux publics aux Pays-Bas et à l'étranger, et donne des informations concernant les aspects techniques de la vidéosurveillance ainsi que des outils pratiques comme une check list et un CD contenant des informations supplémentaires.[30] Le gouvernement belge a pris la même initiative, publiant des directives, des conseils et encourageant les échanges d'expériences.

Au Royaume-Uni, où, ces dernières années, l'expansion de la vidéosurveillance et son efficacité sur la criminalité ont attiré des critiques croissantes (en particulier depuis la publication en 2005 d'une évaluation nationale), le ministère de l'Intérieur et l'Association of Chief Police Officers (Association des Chefs de Police - ACPO) ont publié une *National CCTV Strategy* (Stratégie Nationale pour la Vidéosurveillance) en 2007. Ce document donne un aperçu des 44 recommandations pour des « améliorations potentielles ». Entres autres, il recommande la standardisation de tous les aspects de la vidéosurveillance, la création d'un réseau d'images en direct et enregistrées, la formation de tout le personnel et une meilleure synergie entre les différents acteurs chargés de la gestion de la vidéosurveillance. En outre, il demande d'étendre le pouvoir du Commissionnaire à l'Information de façon à assurer le respect des lois sur l'Informatique et les Libertés. Cette stratégie est soutenue par la mise en place d'une commission nationale de programmes de stratégie pour la vidéosurveillance qui émettra des conseils sur la mise en œuvre des recommandations données dans le rapport et la coordination des activités futures. [31]

La France prend la même direction, son gouvernement travaille actuellement sur une stratégie nationale pour la vidéosurveillance.

La plupart des autres pays européens sont loin de l'élaboration d'approches stratégiques, laissant principalement le développement de la vidéosurveillance aux initiatives locales.

Choix politique ou dynamique technologique ?

Comme nous l'avons vu, le paysage européen de la vidéosurveillance urbaine est caractérisé par une grande diversité en termes de soutien politique, de règlementation juridique, d'organisation, de régimes de protection des données et de stratégies nationales. L'évolution de la vidéosurveillance dans les lieux publics dépend du cadre institutionnel de chaque pays, des ressources financières disponibles et, *last but not least*, du consensus dominant dans le public.

[30] Les directives sont régulièrement mises à jour. La version actuelle est disponible sur : http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/bestuurlijk-handhaven/cameratoezicht/handreiking_cameratoezicht_mei_2009.pdf.

[31] Gerrard, G. et al.. (2007): *National CCTV Strategy.* Londres : Ministère de l'Intérieur.

Toutefois, partout en Europe, le véritable moteur de développement se trouve au niveau local. Les fonctionnaires, les politiciens locaux et la police soutiennent ou empêchent le développement de la vidéosurveillance selon leurs opinions, leurs intérêts et leurs intentions.

Mais dans quelle mesure la politique plutôt que la technologie influence-t-elle l'évolution de la vidéosurveillance ? Les caméras de surveillance ont été utilisées pour le maintien de l'ordre dans les lieux publics depuis plus de 50 ans. Depuis les années 90, il y a eu une expansion massive de la vidéosurveillance qui est présentée comme un outil efficace pour lutter contre la criminalité. Dans un même temps, les études questionnent son efficacité comme une « solution miracle » contre le crime. Aujourd'hui, lors de la justification de la vidéosurveillance dans les débats publics, l'accent est passé de la prévention de la criminalité aux enquêtes judiciaires, où la vidéosurveillance est présentée comme un outil utile pour trouver des preuves lorsqu'un délit est commis.

De nos jours, la vidéosurveillance n'est pas limitée à la prévention de la criminalité. Une fois installé, un système de vidéosurveillance peut être utilisé pour détecter les petits délits tels que l'abandon de détritus et le stationnement non autorisé ou encore pour surveiller les employés municipaux qui travaillent dans les rues. Il peut également être utilisé pour gérer des manifestations publiques importantes ou encore en cas de situation d'urgence majeure.

Une nouvelle tendance se dessine avec la mise en réseau de systèmes anciennement « discrets ». La police et autres agences de maintien de l'ordre demandent un accès en temps réel aux images de vidéosurveillance du réseau de transport d'une ville,

par exemple, ou encore aux images de certains grands organismes publics et privés. De nos jours, l'espace public est couvert par un réseau complexe de systèmes de vidéosurveillance.[32]

Dans l'effort de traiter un nombre croissant d'images, la surveillance algorithmique prend le pas sur les méthodes traditionnelles. Ceci signifie que des décisions vitales sont déléguées à des technologies de biométrie, de reconnaissance automatisée de tendances et à des systèmes d'assistance à la décision basés sur un système SIG sans que l'on en comprenne la teneur exacte. Comme il devient de plus en plus difficile pour les citoyens ordinaires ainsi que pour les décideurs de comprendre la forme et les fonctions actuelles des systèmes de vidéosurveillance semi-automatisés et en réseau, la tendance actuelle soulève de sérieuses questions concernant la transparence et la responsabilité démocratique de la surveillance urbaine actuelle.

L'expansion et l'évolution de la vidéosurveillance en Europe sont arrivées au point où il est maintenant urgent de discuter des principes communs quant à son utilisation, de les développer et de les mettre en œuvre.

---

[32] Le terme est emprunté à McCahill, M. (2002): *The surveillance web. The rise of visual surveillance in an English city*, Cullompton, Devon, UK: Willan Publishing.

L'encadrement juridique de la vidéosurveillance en Europe

Laurent Lim, Conseiller juridique, Commission nationale Informatique et Libertés (France)

Les caméras de surveillance sont aujourd'hui utilisées, de façon plus ou moins massive, dans le monde entier pour contrôler les espaces publics et privés. Accompagnant le mouvement technologique général rendant la captation d'image toujours plus aisée, les systèmes de vidéo surveillance se perfectionnent et évoluent rapidement.

Ainsi, les outils de vidéosurveillance proposent aujourd'hui notamment la transmission des images par Internet (Vidéo IP), des interfaces de gestion s'intégrant en environnement bureautique, une qualité d'image et des capacités de stockage toujours plus performantes. Des outils logiciels de remontée d'alertes sur la base d'une lecture « intelligente » des images sont disponibles et devraient progresser vers des possibilités d'analyses encore plus poussées, et notamment par des utilisations d'images vidéo couplées à d'autres technologies (reconnaissance sonore, reconnaissance faciale).

Ces évolutions futures, la diversification des utilisations, ainsi que la maturité du marché de la vidéosurveillance, mettent au défi les normes juridiques européennes et nationales, que celles-ci encadrent spécifiquement l'utilisation de la vidéosurveillance ou traitent de façon générale la protection des données à caractère personnel.

Si les institutions européennes ont encadré assez tôt la collecte et l'utilisation de données à caractère personnel, les premiers instruments traitant spécifiquement de la question de l'encadrement ne sont apparus que récemment.

Au niveau national, les législations des Etats membres de l'Union européenne, bien que fixant des règles et conditions différentes, permettent le recours à la vidéosurveillance.

En Europe, la question de la conformité de l'utilisation des systèmes de vidéosurveillance à la directive sur la protection des données se pose, et nous verrons qu'il existe des réponses législatives variées dans la façon d'encadrer juridiquement ces systèmes. Il convient de souligner que la loi n'est pas nécessairement le seul instrument juridique pour l'encadrement de la vidéosurveillance : la jurisprudence, les résolutions, avis et recommandations des institutions européennes ou nationales, ainsi que des autorités de protection des données doivent être pris en compte. Enfin, des codes de bonnes pratiques ou chartes éthiques constituent des outils particulièrement utiles à l'auto-régulation.

I. LE CADRE JURIDIQUE EUROPEEN

Certains principes fondamentaux ont été adoptés au niveau européen en matière de protection de droits et libertés fondamentaux, ainsi qu'en matière de protection des données à caractère personnel. Ces textes concernent aussi les traitements des données réalisés dans le cadre d'opérations de vidéosurveillance.

A. Les garanties fondamentales des textes du Conseil de l'Europe

La convention européenne de sauvegarde des droits de l'Homme et des Libertés fondamentales, adoptée à Rome le 4 novembre 1950 par le Conseil de l'Europe

pose dans son article 8 le droit au respect de la vie privée et familiale, du domicile et de la correspondance.
Cette convention a été complétée par un protocole additionnel n°4 du 16 septembre 1963, garantissant dans son article 2 la liberté de circulation pour quiconque se trouve régulièrement sur le territoire d'un Etat.

Par ailleurs, la Convention n°108/1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel adoptée par le Conseil de l'Europe le 28 janvier 1981 et ratifiée par 40 Etats européens, est le premier instrument international contraignant ayant pour objet de fixer des normes minimales pour protéger les personnes contre les abus susceptibles de se produire lors de la collecte et du traitement de données à caractère personnel les concernant.

Elle s'applique aux secteurs public et privé et pose un certain nombre de principes généraux concernant la collecte, le traitement, et la communication de données à caractère personnel par le biais de nouvelles technologies de l'information.

Les activités de vidéosurveillance entrent dans son champ d'application, dans la mesure où elles impliquent le traitement de données à caractère personnel au sens de la Convention n° 108 et où le comité consultatif établi par cette Convention a estimé que les voix et les images doivent être considérées comme des données à caractère personnel lorsqu'elles fournissent des informations sur une personne en la rendant identifiable, même indirectement.

Ces principes portent notamment sur le caractère licite et loyal de la collecte et du traitement automatisé des données personnelles, le principe de leur enregistrement pour des finalités déterminées et légi-

times, la non-utilisation des données à des fins incompatibles avec ces finalités, la limitation de la durée conservation à la durée strictement nécessaire, le caractère adéquat et non-excessif par rapport aux finalités poursuivies, ainsi que la pertinence des données et l'obligation de mise à jour. La Convention proscrit le traitement des données « sensibles » (relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle) et garantit également le droit des personnes concernées de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications.

La Cour européenne des droits de l'Homme a eu l'occasion de préciser les contours de ces garanties en matière de vidéosurveillance. Elle a ainsi la révélation et la publication dans les médias, dans le cadre de campagnes de lutte contre le crime, d'images issues de systèmes de vidéosurveillance de voie publique, à l'insu de la personne filmée, constituent une violation de l'article 8 .

Afin de répondre au besoin de proposer un cadre juridique plus spécifique pour les opérations de vidéosurveillance, et après avoir relevé « avec préoccupation que les lois nationales sont loin d'être homogènes en la matière », l'Assemblée parlementaire du Conseil de l'Europe a adopté le 25 janvier 2008 une résolution n°1604 par laquelle, elle appelle formellement les Etats membres du Conseil de l'Europe à appliquer un ensemble de « principes directeurs pour la protection des personnes vis-à-vis de la collecte et du traitement de données au moyen de la vidéosurveillance ».

Ces principes, au nombre de douze, reprennent et appliquent en matière de vidéosurveillance les principes posés par les instruments du Conseil de l'Eu-

rope, en insistant particulièrement notamment sur la nécessité d'une utilisation pertinente, adéquate et non-excessive par rapport aux finalités ; d'éviter que les données collectées ne soient indexées, comparées ou conservées sans nécessité ; de ne pas se livrer à des activités de vidéosurveillance si le traitement des données à caractère personnel risque d'aboutir à une discrimination contre certains individus ou groupes d'individus uniquement en raison de leurs opinions politiques, de leurs convictions religieuses, de leur santé ou de leur vie sexuelle, ou de leur origine raciale ou ethnique ; d'informer clairement et de façon appropriée les personnes, en indiquant leur finalité ainsi que l'identité des responsables ; de garantir l'exercice du droit d'accès aux images et aux enregistrements ; ainsi que de garantir la sécurité et l'intégrité des images par toute mesure technique et organisationnelle nécessaire.

Le Conseil de l'Europe incite ainsi ses membres à veiller à prévoir dans leur législation nationale des dispositions définissant des restrictions techniques limitant l'installation de ces équipements en fonction du lieu surveillé, les zones privées à exclure du champ de la vidéosurveillance en imposant l'utilisation de logiciels adaptés, le recours en pratique au chiffrement des données vidéo, ainsi que la création de voies de recours juridiques en cas d'allégation d'utilisation abusive de la vidéosurveillance.

Il faut en particulier relever que l'Assemblée parlementaire considère qu'il est nécessaire qu'une signalétique et un texte d'accompagnement uniformisés soient adoptés le plus tôt possible et utilisés par les Etats membres. Au vu des progrès techniques constants en matière de vidéosurveillance, elle souligne la nécessité de poursuivre les travaux sur le thème de la vidéosurveillance à l'avenir.

B. Les autres textes européens

Au titre des autres textes européens pouvant s'appliquer aux activités de vidéosurveillance, il faut en particulier citer la Charte des droits fondamentaux de l'Union européenne. Cette proclamation solennelle, adoptée le 7 décembre 2000 par l'Union européenne, est désormais mentionnée par le traité de Lisbonne du 13 décembre 2007, entré en vigueur le 1er décembre 2009, dans l'article sur les droits fondamentaux. Ceci vise à conférer à la Charte une valeur juridiquement contraignante (sous de fortes restrictions pour certains pays : la Pologne, le Royaume-Uni et la République tchèque).

L'article 7 de la Charte prévoit ainsi que « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

En outre, l'article 8 garantit que « Toute personne a droit à la protection des données à caractère personnel la concernant ». Elle précise encore que « ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi », que « toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification » et que « le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Il faut également signaler que le Contrôleur européen de la protection des données (CEPD), qui a compétence pour superviser les traitements de données à caractère personnel mis en œuvre par les institutions européennes, a publié le 17 mars 2010 un ensemble de lignes directrices sur la vidéosurveillance, à destination des institutions et organes européens.

Ces lignes directrices détaillées, élaborées à l'issue d'un processus de consultation, comportent un certain nombre de recommandations pratiques. Elles mettent notamment en avant le concept de « privacy by design », selon lequel les garde-fous techniques permettant de mieux protéger les données à caractère personnel et la vie privée des personnes filmées doivent être incorporés, dès la conception, dans les spécifications technologiques.

C. La Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Cette Directive constitue l'instrument juridique adopté par l'Union européenne pour fixer les principes de protection des données à caractère personnel des citoyens européens. C'est sur la base de ce texte que les Etats membres ont adopté des législations nationales sur la protection des données.

La Directive est en principe applicable aux systèmes de vidéosurveillance, dès lors qu'elle s'applique à toute information, y compris sous forme de sons et images, concernant une personne identifiée ou identifiable, en tenant compte de l'ensemble des moyens pouvant être raisonnablement utilisés par le responsable de traitement ou par d'autres personnes afin d'identifier ladite personne.

En effet, les images et sons qui se rapportent à des personnes physiques identifiées ou identifiables sont considérés comme des données à caractère personnel même si les images sont utilisées dans le cadre de la vidéosurveillance, même si elles ne sont

pas associées aux données d'identité de la personne et même si elles ne concernent pas de personnes dont le visage a été filmé, bien qu'elles contiennent d'autres informations (par exemple, le numéro de la plaque d'immatriculation de son véhicule).

Toutefois, la vidéosurveillance des lieux publics ne relève que partiellement de la Directive 95/46, dans la mesure où elle n'est pas applicable au traitement de données sous forme de sons et d'images réalisé pour des finalités de sécurité publique, la défense, la sûreté de l'Etat, pour l'exercice d'activités de l'Etat dans le domaine du droit pénal, ou pour d'autres activités qui ne tombent pas dans le champ d'application du droit communautaire.

Par ailleurs, la Directive n'est pas applicable aux traitements effectués par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques.

Le groupe au niveau européen des autorités nationales de protection des données (dit « Groupe de l'article 29 » ou « G29 ») a ainsi précisé, dans un avis de 2004 , l'interprétation des dispositions de la directive n° 95/46.

Cet avis souligne en particulier la nécessité que les institutions concernées des Etats-membres mènent d'une part une évaluation générale de la vidéosurveillance afin « d'éviter qu'une excessive prolifération des systèmes d'acquisition d'images en des endroits publics et privés n'entraîne une restriction injustifiée des droits et libertés fondamentaux des citoyens » qui rendrait ces derniers « massivement identifiables dans un grand nombre de lieux publics et privés » ; ainsi qu'une évaluation de l'évolution

des techniques de vidéosurveillance, afin d'éviter que le développement de logiciels de reconnaissance du visage des personnes et de détection/prévision comportementale « n'entraîne un passage massif et inconsidéré à une surveillance du type dynamique-préventive ».

Ces deux messages demeurent d'actualité. La définition d'outils et méthodes les plus fiables possibles pour évaluer l'efficacité de la vidéosurveillance demeure cruciale et indispensable.

II. LES LEGISLATIONS NATIONALES

A. La diversité des systèmes de régulation

En différents Etats membres, il existe déjà des cas d'études en matière de vidéosurveillance, qui reposent sur des normes constitutionnelles ou sur des dispositions législatives spécifiques, des prescriptions ou d'autres décisions émanant des autorités nationales compétentes.

Dans certains pays, il existe également des dispositions spécifiques qui s'appliquent indépendamment du fait que la vidéosurveillance comporte ou non le traitement de données à caractère personnel. Ces dispositions prévoient également que l'installation et la mise en œuvre d'un système de vidéosurveillance soient soumises à autorisation préalable de la part d'une autorité administrative, qui peut être représentée, en tout ou en partie, par l'autorité nationale pour la protection des données à caractère personnel. Les règles peuvent varier selon la nature publique ou privée de la personne responsable du fonctionnement de l'installation.

Dans d'autres pays, la vidéosurveillance ne fait pas l'objet de dispositions de loi spécifiques. Dans certains cas toutefois, les autorités de protection des données à caractère personnel ont pu jouer leur rôle au moyen d'avis, de lignes directrices ou codes de conduite (Royaume Uni, Italie), afin de garantir une application appropriée des dispositions générales de protection des données.`

L'avis du G 29 du 11 février 2004 précité comporte un tableau récapitulatif des principales sources juridiques nationales en matière de vidéosurveillance connues au sein des Etats-membres au jour de son adoption.

AVERTISSEMENT : Ce tableau, repris ci-dessous à titre d'information, ne peut être considéré comme exhaustif s'agissant des éventuels textes nouveaux qui auraient pu intervenir postérieurement au 11 février 2004.

Allemagne

Article 6, point b de la loi fédérale 2000
Article 25 de la loi sur la protection des frontières.
Autres réglementations en matière de vidéosurveillance exercée par la police dans les législations des Länder sur la police.

Belgique

Avis de l'Autorité chargée de la protection des données, en particulier avis d'initiative 34/99 du 13 décembre 1999, relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéosurveillance ;
avis d'initiative 3/2000 du 10 janvier 2000 relatif à l'utilisation de systèmes de vidéosurveillance dans les halls d'immeubles à appartements ;
loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance.

Danemark
Loi de synthèse n° 76 du 1er février 2002 relative à l'interdiction de la vidéosurveillance. Cette loi interdit d'une façon générale aux entités privées d'exercer une vidéosurveillance sur la voie publique et dans les squares ou toute zone équivalente de libre circulation, tout en aménageant toutefois certaines dérogations à cette interdiction.
Décision de l'Autorité chargée de la protection des données du 3 juin 2002 concernant la vidéosurveillance par un grand groupe de supermarchés et transmission directe sur Internet depuis un café.
Décision de l'Autorité chargée de la protection des données du 1er juillet 2003 selon laquelle la vidéosurveillance exercée par une société privée de transport public doit être adaptée et conforme aux dispositions de la loi sur la protection des données.
Décision de l'Autorité chargée de la protection des données du 13 novembre 2003 imposant certaines restrictions à la vidéosurveillance exercée par les pouvoirs publics
Deux lois ont été adoptées en matière de vidéosurveillance en juin 2007 : la première donne aux entreprises privées le pouvoir d'opérer une surveillance des zones dont elles sont propriétaires, sans obligation de déclaration préalable à l'autorité de protection des données, la seconde donne aux services police des pouvoirs accrus permettant d'imposer à des administrations ou à des organismes privés l'installation et la mise en œuvre de systèmes de vidéosurveillance.

Espagne
Ley organica n° 4/1997 (vidéosurveillance par les forces et les corps de sécurité en des lieux publics)
Real Decreto n° 596/1999 d'application de la loi n° 4/1997

Finlande
En Finlande, il n'existe pas de législation spéciale en matière de vidéosurveillance mais des dispositions d'un grand nombre de textes législatifs différents s'appliquent à la vidéosurveillance ainsi qu'à d'autres systèmes de surveillance, d'observation et de contrôle techniques.
Le médiateur pour la protection des données a rendu un avis sur l'enregistrement des conversations téléphoniques par les services de la clientèle et dans le milieu de travail (numéros de dossier 1061/45/2000 et 525/45/2000).

France
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (CNIL).
La loi n° 95-73 du 21 janvier 1995 relative à la sécurité (modifiée), décret n° 96-926 du 17 octobre 1996 (modifié) et la circulaire du 22 octobre 1996 (modifié) sur la mise en œuvre de la loi n° 95-73 encadrent par un régime spécifique d'autorisation préfectorale la mise en œuvre de systèmes de vidéosurveillance aux fins de sécurité dans les lieux publics.
La Commission nationale de l'informatique et des libertés (CNIL), autorité chargé de la protection des données, a publié un Guide comportant des recommandations concernant la vidéosurveillance sur le lieu de travail.

Grèce
Lettre n°390 du 28 janvier 2000 concernant l'installation d'un système de télévision en circuit fermé dans le Métro d'Athènes.
Directive n°1122 du 26 septembre 2000 concernant la télévision en circuit fermé.
Décision n°84/2002 relative aux systèmes de télévision en circuit fermé dans les hôtels.

Irlande
Loi sur la protection des données de 1998 et de 2003
Étude de cas nº 14/1996 (utilisation de la CCTV)

Italie
Article 34 du code de protection des données à caractère personnel (D.lg. nº196 du 30 juin 2003 portant adoption du code de conduite)
Décisions de l'autorité de contrôle (Garante) nº 2 du 10 avril 2002 (promotion du code de conduite); 28 septembre 2001 (techniques biométriques et reconnaissance du visage près les banques) et 29 novembre 2000 (le « décalogue » sur la vidéosurveillance) d.P.R. 22 juin 1999, nº 250 (accès des véhicules aux centres historiques et aux zones à circulation limitée)
D.l. 14 novembre 1992, nº 433 et l. n. 4/1993 (musées, bibliothèques et archives de l'Etat)
D.lg. 4 février 2000, nº 45 (paquebots affectés à des voyages nationaux)
Article 4 l. 20 mai 1970, nº 300 (Statut des travailleurs)

Luxembourg
Articles 10 et 11 de la loi du 02.0802002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Pays-Bas
Le rapport de l'autorité chargée de la protection des données publié en 1997 contient des lignes directrices concernant la vidéosurveillance, en relation notamment avec la protection des personnes et des biens dans les lieux publics.
Enquête sur la vidéosurveillance dans l'ensemble des municipalités néerlandaises en 2003.
Modification du code pénal entrant en vigueur à compter du 1er janvier 2004 et étendant le champ

d'application de l'infraction consistant à photographier des lieux accessibles au public sans en informer les personnes

Portugal
Décret-loi 231/98 du 22 juillet 1998 (activités privées de sécurité et systèmes d'autoprotection)
Loi 38/98 du 4 août 1998 (mesures à adopter en cas de violence associée à des événements sportifs)
Décret-loi 263/01 du 28 septembre 2001 (discothèques)
Décret-loi 94/2002 du 12 avril 2002 (événements sportifs)

Royaume-Uni
CCTV Code of practice (Information Commissioner) revise en 2008

Suède
La vidéosurveillance est spécifiquement réglementée par la loi (1998:150) relative à la vidéosurveillance générale et la loi (1995:1506) sur la vidéosurveillance secrète (dans les enquêtes criminelles).
La vidéosurveillance générale requiert en principe l'autorisation d'une administration régionale bien qu'il y ait un certain nombre d'exceptions, par exemple, en ce qui concerne la surveillance des bureaux de poste, des banques et des magasins. La vidéosurveillance secrète doit être autorisée par un tribunal. Le Chancelier de la Justice peut faire appel d'une décision de la commission administrative régionale.
L'enregistrement vidéo par des caméras numériques est considéré comme un traitement de données à caractère personnel et est donc placé sous la supervision de l'autorité chargée de la protection des données dans la mesure où elle n'est pas spécifiquement réglementée par la loi relative à la vidéosurveillance générale.

Une commission d'enquête a publié en 2002 un rapport sur la vidéosurveillance (SOU 2002 :110).

Les autres instruments qui méritent d'être mentionnés concernent l'Islande (article 4, loi nº 77/2000), la Norvège (titre VII loi nº 31 du 14 avril 2000), la Suisse (recommandation du Responsable fédéral) et la Hongrie (recommandation DPA du 20 décembre 2000).

B. Vers une législation européenne spécifique ?

Cette diversité des législations, combinée aux rapides avancées technologiques des systèmes conforte la pertinence d'une approche juridique plus harmonisée. Plusieurs travaux récents au niveau européen s'inscrivent en effet dans cette optique et recommandent le renforcement des législations européennes et nationales.

Dans son rapport du 7 mai 2010 sur le rôle des autorités de protection des données en Europe, l'Agence européenne des droits fondamentaux retient le développement des systèmes de vidéosurveillance comme un point de préoccupation nécessitant une action urgente : « La vidéosurveillance des lieux publics est largement répandue, mais l'encadrement législatif est à la traîne. Le rapport révèle par exemple que souvent en pratique, les caméras de vidéosurveillance ne sont pas déclarées et/ou ne sont soumises à aucun contrôle dans certains Etats membres ».
Le rapport précise ainsi qu'en Autriche, la vaste majorité des caméras ne sont pas déclarées (et échappent ainsi au contrôle de l'autorité de protection des données), qu'en Allemagne certains cas de vidéosurveillance à l'insu des salariés sur leur lieu de travail ont été signalés. Il rappelle qu'en Grèce, l'Autorité de

protection des données s'est vue refuser l'accès aux locaux de la police dans lesquels des traitements de données étaient effectuées, et qu'au Royaume-Uni, il existe peu de restrictions sur l'utilisation de caméras dans l'espace public, et qu'il existe dans cet Etat-membre plus de caméras que nulle part ailleurs dans le monde.

L'Agence des droits fondamentaux estime ainsi que, tout en ayant à l'esprit les particularités techniques intrinsèques des données sonores et visuelles, ainsi que l'impact potentiellement important sur les droits des individus, un instrument législatif européen spécifique devrait être envisagé dans le futur.
Enfin, le Conseil de l'Europe, dans son projet de recommandation sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre de traitements de « profilage » adopté le 15 juin 2010 , constate que la collecte et le traitement des données à des fins de profilage peuvent utiliser différents types de données, telles que celles « provenant des systèmes de vidéosurveillance ».

En l'absence d'initiative législative européenne visant à encadrer de façon spécifique les opérations de vidéosurveillance, les acteurs peuvent s'appuyer sur les avis ou recommandations sectorielles des autorités nationales de protection des données.

Certains choisissent, dans le souci d'assurer le meilleur encadrement juridique et l'utilisation la plus cohérente possible de leur système de vidéosurveillance, de se doter d'une charte éthique fixant des règles de bonne conduite et de bonne gestion. C'est dans cette optique que s'inscrit la Charte proposée par le Forum européen sur la Sécurité urbaine dans le cadre du projet « Citoyens, villes et vidéosurveillance ».

Partie II

➤ *Vers une charte pour une utilisation démocratique de la vidéosurveillance dans les villes européennes*

« J'appelle les élus à étudier et signer la *Charte pour une utilisation démocratique de la vidéosurveillance* »

Un entretien avec Charles Gautier, sénateur-maire de Saint-Herblain et président du Forum français pour la Sécurité urbaine

➤ **Vous êtes l'un des deux premiers signataires, avec le maire de Rotterdam, de la nouvelle *Charte pour une utilisation démocratique de la vidéosurveillance.***

Pourquoi cette Charte ?

Charles Gautier : Cette Charte est issue d'un travail qui a été mené à l'échelle européenne par un ensemble de villes et d'acteurs impliqués dans la vidéosurveillance.

Depuis une quinzaine d'années, la vidéosurveillance urbaine a connu un essor très important en Europe, bien qu'il y ait des différences significatives d'un pays à l'autre autant en ce qui concerne la densité des réseaux installés qu'en ce qui concerne les législations et modalités de contrôle. Aujourd'hui, nous en sommes arrivés à un point où il est devenu nécessaire de réfléchir en commun sur cette technologie qui n'est pas anodine puisqu'elle entraîne de facto une ingérence dans la vie privée des citoyens, filmés à leur insu dans les rues de nos villes.

L'Efus a donc lancé un projet européen autour de cette question, dans lequel le Forum français a joué un rôle d'expert. L'objectif était de débattre en commun sur les implications politiques et sociales de la vidésurveillance urbaine. Comment utiliser cette technologie ? Quel cadre légal et politique ? Comment garantir le respect des libertés ? Qui contrôle ? Qui surveille ? Qui surveille-t-on ? Quelles experiences menées dans telle ou telle ville ou pays

peuvent être appliquées ailleurs ? Quels enseignements tirer des « mauvaises » expériences ?
La *Charte pour une utilisation démocratique de la vidéosurveillance* reprend les thèmes-clés sur lesquels nous avons travaillé et surtout, elle présente un certain nombre de principes fondateurs pour, comme son titre l'indique, une utilisation démocratique de la vidéosurveillance dans le respect des libertés fondamentales des citoyens.

A qui s'adresse la Charte et à quoi sert-elle ?
Il faut tout d'abord préciser que cette Charte n'est en aucun cas un document réglementaire qui imposerait un certain nombre de directives aux villes européennes. Elle a été conçue et rédigée par les villes elles-mêmes pour mettre au clair un certain nombre d'idées communes. C'est donc un outil mis à la disposition des villes pour les aider à définir d'une part la place de la vidéosurveillance dans leur politique de sécurité urbaine et d'autre part les modalités pratiques de son utilisation. C'est une sorte de guide, si vous voulez. C'est aussi une déclaration de principes.

A quel titre avez-vous participé à ce projet ?
Tout d'abord en ma qualité de sénateur-maire de Saint-Herblain, l'une des dix villes partenaires de ce projet. Saint-Herblain est une ville de 45.000 habitants située dans l'agglomération de Nantes, en Loire Atlantique, au nord-ouest de la France. L'agglomération nantaise compte 500.000 habitants.
Saint-Herblain a installé les premières caméras de vidéosurveillance en 1999. Il y en a aujourd'hui 18. En tant que maire, j'ai une ligne politique claire : concilier l'exigence de sécurité des citoyens avec le respect des libertés individuelles. Le développement de notre système de vidéosurveillance se fait en fonction de ce choix stratégique.
J'ai également participé à ce projet en ma qualité de sénateur puisque j'ai été co-rapporteur, avec le sénateur Jean-Patrick Courtois, d'un rapport d'information au Sénat sur la vidéosurveillance. Nos recommandations se situent dans la même ligne que les principes définis dans le projet européen « Citoyens, villes et vidéosurveillance ».
Enfin, j'ai été associé au projet en ma qualité du président du Forum français, où nous avons également mené des réflexions autour de ce sujet avec les élus.

La vidéosurveillance est-elle un thème important pour les élus en France ?
Sans aucun doute. Non seulement parce que la vidéosurveillance est un élément important dans la politique de sécurité des villes, mais aussi parce qu'il y a une volonté politique à l'échelle nationale. Le gouvernement a annoncé que, dans le cadre de la lutte contre le terrorisme, son objectif était de tripler le nombre de caméras installées en France d'ici à la fin 2011, pour atteindre un total de 60.000.
D'importants investissements sont consacrés à la vidéosurveillance. Ainsi, une bonne part du Fonds interministériel de Prévention de la délinquance est dédiée à son financement. Elle est également financée par les départements, qui y consacrent une part importante de leur dotation : pas moins de 30 millions d'euros sur un total de quelque 49 millions en 2010.

Quelle est la position du Forum et des élus français sur cette question ?
Nous n'avons pas de position dogmatique au sein de notre réseau. Mais ce qui est certain, c'est que de nombreuses collectivités cherchent aujourd'hui à évaluer l'efficacité de la vidéoprotection et surtout, à concilier cette technologie avec le respect des libertés fondamentales.
Il y a beaucoup de discussions autour de ces thèmes.

Pour résumer, disons qu'il y a un consensus général autour de quatre grands principes.
Premièrement, la vidéosurveillance est un outil qui doit être utilisé dans le cadre d'une politique globale de prévention de la délinquance. Il est important de prendre en compte non seulement les aspects techniques mais aussi l'organisation, les ressources humaines, le coût financier et la dimension éthique.
Deuxièmement, il nous paraît fondamental que les municipalités investissent dans la formation des opérateurs. Non seulement sur l'utilisation technique des systèmes mais aussi sur les objectifs de la municipalité. Les opérateurs doivent connaître la politique locale de sécurité et de prévention de la délinquance et les objectifs de la mairie. Ils doivent aussi connaître la réglementation en vigueur, notamment en ce qui concerne le respect de la vie privée et des libertés individuelles.
Troisième principe : l'importance de mettre en place une méthode d'évaluation du système local de vidéosurveillance en fonction des objectifs qui lui ont été assignés. Ces systèmes coûtent cher aux collectivités. Il nous paraît donc indispensable qu'elles aient des outils d'évaluation, notamment pour garantir une bonne cohérence entre le système vidéo et les autres dispositifs locaux de sécurité et, si besoin, faire les améliorations nécessaires.
Enfin la quatrième idée-force est que tout système de vidéoprotection doit être utilisé dans le respect des règles éthiques. Deux notions nous paraissent particulièrement importantes : l'utilisation transparente de ces systèmes et la « traçabilité » des informations recueillies.

Vous êtes, avec le maire de Rotterdam (Pays-Bas), l'un des premiers signataires de la *Charte pour une utilisation démocratique de la vidéosurveillance*. Qu'apporte-t-elle de nouveau ?

Il n'existe à ce jour aucun texte européen sur la vidéosurveillance. Cette Charte est donc une première. Elle est issue de la volonté d'un certain nombre de villes européennes de se doter d'un cadre de référence. Si les maires ont éprouvé ce besoin, c'est bien parce qu'ils sont directement en prise avec les attentes des habitants des villes en matière de sécurité mais aussi de leurs craintes quant au respect de leur vie privée. C'est donc tout le contraire d'une approche bureaucratique, qui serait partie d' «en haut».
Cette Charte nous donne, à nous les élus locaux, des critères d'évaluation et des recommandations concrètes dans le cadre des réglementations européennes et nationales actuelles. Ce n'est pas une déclaration en faveur ou contre la vidéosurveillance.

Vous avez appelé vos collègues maires et élus locaux européens à signer cette Charte. Qu'est-ce que cela change, concrètement, d'être signataire ?
J'appelle les élus non seulement à signer mais aussi à étudier la *Charte pour une utilisation démocratique de la vidéosurveillance* parce que je crois qu'elle aborde un thème essentiel et urgent.
Aujourd'hui, vu l'expansion des systèmes de vidéosurveillance et leur évolution technologique, tout maire ou représentant de collectivité locale, même relativement petite, est amené à gérer de tels systèmes, donc à prendre position.
Cette Charte permet aux élus qui le souhaitent de s'approprier un certain nombre de principes qui garantissent l'utilisation démocratique de la vidéosurveillance. Signer la Charte, cela signifie que l'on s'engage publiquement envers les citoyens de la ville ou collectivité locale dont on est l'élu à garantir le respect de leurs libertés fondamentales.

LA VIDÉOSURVEILLANCE EN FRANCE : CHIFFRES CLÉS

➤ La France compte **396 000** caméras autorisées dont 20 000 sur l'espace public (chiffre 2007)

➤ **9772** autorisations ont été délivrées pour l'année 2007 aux opérateurs publics et privés (soit une hausse de 5 % par rapport à 2006) dont 86 % concernent des systèmes installés dans des lieux ou établissements ouverts au public et 14 % des systèmes visionnant la voie publique. *Note: 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. A l'inverse, des autorisations sont accordées, mais les caméras ne sont pas nécessairement installées.*

➤ **1522** communes françaises (sur un total de 36 682 au 1er janvier 2009, selon l'Institut national de la statistique et des études économiques) utilisent au moins un système de vidéosurveillance.

LES FRANÇAIS TRÈS LARGEMENT FAVORABLES À LA VIDÉOSURVEILLANCE

Selon un sondage réalisé en 2008, 71 % de la population française est favorable à l'utilisation de la vidéosurveillance dans les lieux publics, contre 28% qui s'y opposent.

A la question, « De façon générale, êtes-vous très favorable, plutôt favorable, plutôt défavorable ou très défavorable à la présence de caméras de vidéosurveillance dans les lieux publics ? »

➤ **21 %** se déclarent très favorables

➤ **50 %** plutôt favorables

➤ **15 %** plutôt défavorables

➤ **13 %** très défavorables

➤ **1 %** ne savent pas

Ce sondage a été réalisé du 14 au 17 mars 2008 par la société Ipsos, pour le compte de la Commission nationale Informatique et Libertés (CNIL), auprès d'un échantillon de 972 personnes représentatif de la population française âgée de 18 ans et plus.

II. Pourquoi (des recommandations sous la forme d') une charte ?

A travers le projet « Citoyens, villes et vidéosurveillance », le Forum européen pour la Sécurité urbaine a souhaité initier une réflexion et un échange d'expériences sur les pratiques de la vidéosurveillance dans le respect et la protection des libertés individuelles. A travers trois visites d'études à Gênes (Italie), Londres et Brighton (Royaume Uni) ainsi qu'à Lyon (France), et les expériences des partenaires du projet. Ce travail a permis d'obtenir une vue d'ensemble des pratiques de la vidéosurveillance et des moyens mis en place pour garantir le respect des droits des citoyens.

Que peut-on conclure de ce projet ? Quels enseignements tirer des expériences et du savoir-faire acquis par les villes ? Quels conseils peut-on donner aux villes partenaires de l'Efus et au-delà, à l'ensemble des acteurs concernés par la vidéosurveillance ? Peut-on recommander des bonnes pratiques ?

Des principes-clés pour concilier la vidéosurveillance et la protection des droits fondamentaux

Certes, le projet a identifié des pratiques que les partenaires ont qualifié de « bonnes » lorsqu'elles sont appliquées pour un problème donné, dans un contexte spécifique. Au début du projet, les partenaires ont développé ensemble une grille de lecture afin d'évaluer les différentes pratiques avec les mêmes critères et en posant chaque fois les mêmes questions : protection des données, garde-fous garantissant le respect de la vie privée, implication des citoyens à toutes les étapes d'un projet de vidéosurveillance - conception, mise en oeuvre, utilisation,

évaluation et développement du système. Toutefois, les partenaires ont estimé qu'il était difficile de recommander à toutes les villes d'appliquer telle ou telle pratique conçue et mise en place par une ville en particulier, en fonction d'un contexte spécifique. En effet, le projet a montré qu'il n'existe pas de bonne pratique européenne, mais qu'en revanche, il est intéressant d'échanger de multiples idées et pratiques pour que chacun détermine le chemin à suivre pour atteindre l'objectif commun à tous, qui est celui de la protection des droits individuels.

Il fallait donc dans un premier temps identifier les principes généraux sur lesquels les bonnes pratiques sont fondées. Dans un deuxième temps, les différents enjeux de la vidéosurveillance ont été examinés. Enfin, des idées de pratiques ont été formulées pour mettre en oeuvre ces principes en tenant compte de ces enjeux préalablement identifiés.

L'idée d'une *Charte pour l'utilisation démocratique de la vidéosurveillance* qui se veut universelle et formule les principes de base qui devraient gouverner la vidéosurveillance est née d'une triple réflexion :

1) Des principes qui peuvent s'appliquer à la vidéosurveillance partout en Europe

Dans une réflexion européenne sur l'utilisation de la vidéosurveillance dans le respect des droits fondamentaux, il est nécessaire de trouver un dénominateur commun qui peut guider les utilisateurs au-delà des différents contextes institutionnels, légaux et culturels. Il ne s'agit pas d'aboutir au plus petit dénominateur commun, mais bien au contraire de trouver les points essentiels sur lesquels tout le monde est d'accord, sachant que chacun a ensuite tout loisir de s'appuyer sur un large éventail d'op-

tions pour adopter la ou les solutions les plus adaptées à chaque pays ou région, en fonction de chaque situation.

2)Des principes qui peuvent être appliqués à tous les enjeux de la vidéosurveillance

L'objectif de la charte est de formuler un ensemble de normes qui répondent à tous les enjeux de la vidéosurveillance. Les partenaires ont ainsi cherché à identifier les principes fondamentaux qui fondent le droit au respect de la vie privée dans tous les aspects de l'utilisation de la vidéosurveillance. Ces principes sont indépendants les uns des autres et complémentaires. Ils peuvent être appliqués dans tous les cas de recours à la vidéosurveillance, que ce soit la planification d'un projet, la mise en oeuvre d'un système, son mode d'utilisation, la protection des données, ou encore l'évaluation du système et les éventuelles modifications. C'est dans l'application de ces principes que les recommandations sur le type d'actions à mener apparaissent. Ensuite, les exemples des pratiques et techniques concrètes peuvent inspirer la mise en œuvre d'actions.

3)Des principes durables dans un contexte de développement technologique rapide

L'évolution technologique et l'accroissement permanent de la capacité des systèmes de vidéosurveillance ont constitué un thème-clé des débats sur la protection de la vie privée. En effet, les systèmes sont de plus en plus puissants et intelligents (reconnaissance automatique des véhicules, des personnes, des comportements, etc.) et ils sont aussi de plus en plus souvent connectés à d'autres systèmes d'information. La vidéosurveillance n'est qu'un élément parmi d'autres au sein du maillage technologique

qui régit nos villes et qui se développe irréversiblement, à une vitesse exponentielle. C'est pourquoi toute recommandation sur la bonne utilisation de la vidéosurveillance peut être vite dépassée par la réalité technologique.

D'autre part, l'évolution des technologies offre de nouvelles solutions à certains dilemmes éthiques. Par exemple il existe aujourd'hui des systèmes qui empêchent les caméras de filmer l'intérieur des espaces privés (voir l'article de Jeroen van den Hoven), C'est pourquoi les recommandations formulées dans la Charte ne traitent pas des méthodes pratiques d'utilisation de telle ou telle technique, mais de l'application de principes de fond.

Il n'en reste pas moins que l'un des objectifs de ce travail était aussi de donner aux villes des moyens concrets pour agir. C'est pourquoi la charte présente, à titre indicatif, un certain nombre de recommandations et de méthodes pratiques.

Il est important aussi de signaler que la *Charte pour une utilisation démocratique de la vidéosurveillance* ne prétend pas résumer l'ensemble des débats qui ont eu lieu dans le cadre du projet. Toutefois, la charte ne peut et ne veut se substituer à l'échange des pratiques concrètes qui s'est fait dans le cadre du projet dont cette publication est le récit. La publication est un complément à la charte et se veut un premier pas vers un guide pratique.

Une charte européenne des villes et régions

L'élaboration de la charte ne s'est pas faite uniquement sur la base des pratiques recueillies auprès des villes. Bien évidemment, les débats se sont aussi fondés sur les législations nationales en vigueur, les

textes européens et les premières initiatives de chartes locales traitant de la garantie du respect des droits individuels.

L'initiative menée ici par l'Efus n'est pas la seule dans son genre. Il s'agit plutôt d'un travail complémentaire, qui comble un vide à la fois local et européen. La vidéosurveillance est un phénomène européen qui concerne tous les citoyens qui vivent, travaillent et voyagent en Europe. En même temps, la vidéosurveillance de l'espace public relève de la responsabilité des autorités locales. L'originalité de la charte est qu'elle établit un pont entre les dimensions locale et européenne.

En effet, les textes européens traitant de la vidéosurveillance ne peuvent fournir que des avis et recommandations d'experts. Une charte des collectivités locales européennes reflète, elle, l'engagement d'un ensemble de villes et de régions de toute l'Europe à respecter, localement, les principes garantissant une utilisation démocratique de la vidéosurveillance.

Les institutions européennes jouent un rôle important dans la protection des droits fondamentaux et la protection de la vie privée : Convention des droits de l'Homme du Conseil de l'Europe (1950) article 8, Charte des droits fondamentaux de l'Union européenne (2001/2009) article 7 et 8, et, dans la protection des données, Convention 108 1981 du Conseil de l'Europe, Directive 95/46/CE de l'Union européenne. Elles ont aussi pris position sur la question de la vidéosurveillance et formulé des recommandations très similaires à celles de la charte aux nôtres dans le rapport du Comité européen de Coopération juridique (CDCJ) (2003), l'Avis 4/2004 du Groupe de travail Article 29, de la Commission de Venise (2007), dans la résolution 1604 (2008) de

l'Assemblée Parlementaire du Conseil de l'Europe, et les lignes directrices sur la vidéosurveillance du Contrôleur européen de la protection des données (CEPD) (2010).

Ces textes très complets ayant beaucoup inspiré le projet n'ont pas pour autant explicité les principes sur lesquels ces recommandations diverses sont fondées. Bien que plusieurs pays aient saisi l'occasion de la transposition de la directive 95/46/CE en droit national pour légiférer aussi sur la vidéosurveillance et que les conventions sur la sauvegarde des droits fondamentaux et de la protection relèvent du droit européen et international, les institutions européennes n'ont pour l'instant pas de compétence pour légiférer sur la vidéosurveillance. Elles doivent se contenter des avis et des recommandations et compter sur le fait que leur message est reçu, ainsi que sur la bonne volonté des parties prenantes. C'est justement en l'absence de réglementation européenne que la charte du Forum prend tout son sens. En ce qui concerne les législations nationales qui, elles, dictent le cadre contraignant pour l'utilisation de la vidéosurveillance, elles varient beaucoup d'un pays à l'autre (voir l'article de Laurent Lim dans ce volume). Tandis que certains pays ont des législations et des réglementations très précises pour la vidéosurveillance d'autres sont restés avec une législation générale de protection de la vie privée et des données personnelles. Dans certains pays, une charte sur la vidéosurveillance apporterait donc une nouveauté. Dans beaucoup d'autres, les principes de la charte complèteront la législation en place et surtout souligneraient une volonté et un souci politiques pour une utilisation responsable de cette technologie de la part des autorités et élus territoriaux.

L'engagement des villes dans la charte – un complément important à la législation en place. [1]

Les chartes et codes de bonne conduite sont des formes de régulations informelles ou de « soft law » puisqu'ils ne constituent pas une législation officielle. Cependant, on aurait tort de penser que ces chartes ne sont pas importantes pour la régulation interne. En fournissant des valeurs et des principes de gestion, elles peuvent jouer un rôle pivot dans la création d'une culture organisationnelle de la vidéosurveillance et apporter des principes aux opérateurs de caméras et aux responsables, qui peuvent les guider dans la prise de décision au quotidien. De plus, elles peuvent aussi servir de point de référence (benchmark) pour mesurer la performance du système et fournir la base pour le développement de procédures détaillées concernant l'opération et la gestion d'un centre de vidéosurveillance.

Les chartes peuvent également jouer un rôle important dans la communication envers le public. En procurant une explication claire sur la raison d'être et les limites de l'installation de vidéosurveillance, une charte peut rassurer sur la finalité du système et apporter au public un certain nombre de critères pour évaluer le bon fonctionnement et le succès du système. Dans ce sens, elles peuvent fournir aux citoyens un cadre clair dans lequel ils peuvent exprimer leurs inquiétudes. Un tel cadre peut par conséquent aider les citoyens à vérifier que les responsables du système assument leurs responsabilités et ne dépassent leur mandat « de surveillance ».

En ce qui concerne la relation entre les chartes et le pouvoir discrétionnaire de l'exécutif local, il est clair que l'importance de la « soft law » dépend des circonstances et des besoins locaux. Il existe dans plu-

sieurs villes européennes la conception que les installations de vidéosurveillance devraient être sous le contrôle direct des élus locaux et que leur fonctionnement devrait faire partie de leur pouvoir discrétionnaire. Evidemment, comme les chartes ne sont pas légalement contraignantes ou opposables, elles ne peuvent se substituer au pouvoir discrétionnaire de l'exécutif. Elles ne peuvent pas non plus être utilisées pour modifier ou interpréter des lois existantes. Cependant, l'adoption d'une charte aurait l'avantage de fournir une structure pour l'utilisation du pouvoir discrétionnaire, de donner de la transparence dans l'utilisation de la vidéosurveillance et d'assurer que ses objectifs sont bien connus et compris par le public. Enfin, des chartes peuvent aider de nouveaux élus à comprendre le fonctionnement et les enjeux de la vidéosurveillance et à garantir un certain degré de continuité opérationnelle et de gestion, après des élections ou pendant d'autres périodes de changement politique.

En résumé, l'avantage principal des chartes est leur capacité à créer des pratiques organisationnelles et opérationnelles, de promouvoir la responsabilité (accountability) et de la transparence et de favoriser ainsi la compréhension de la vidéosurveillance par le public. C'est pour ces raisons qu'elles peuvent être un atout très utile pour les lois et régulations existantes et faire pendant à la gestion de la vidéosurveillance exercée par le pouvoir exécutif discrétionnaire et l'administration. C'est pour ces raisons que plusieurs membres de l'Efus tels Lyon, Le Havre se sont déjà dotés d'une charte. C'est pourquoi aussi la Commission nationale (française) de l'Informatique et des Libertés (CNIL) a accompagné cette initiative

[1] Cette partie Benjamin Goold, Université de British Columbia/ Université d'Oxford.

et contribué à une initiative similaire auprès du groupe Art 29, une initiative appréciée par le Contrôleur européen de la protection des données (CEPD). Ainsi, les partenaires du projet estiment que toute initiative de création d'une charte peut intéresser non seulement les villes et régions européennes mais également tous les acteurs qui ont des objectifs similaires.

3. Les principes de la Charte

1. Le principe de légalité

Le Forum s'est constitué autour d'une conviction - « les villes aident les villes » - qui inspire tous les projets européens qu'il développe. Dans la réflexion autour de la thématique centrale du projet sur la vidéosurveillance, chaque ville partenaire a exprimé la volonté de connaître l'expérience et le contexte des autres villes du projet.

Ceux-ci sont avant tout déterminés par la législation en vigueur. Evoquer un principe de légalité n'est pas venu comme une évidence. En effet, fallait-il parler de légalité ou plutôt de légitimité ?

La légitimité, c'est être en droit de mener une action ou d'occuper une position. Par exemple les élus tirent leur légitimité des élections ou les policiers d'un statut que leur confère un concours. La seule légitimité qui s'applique à tous les cas est celle de la loi. Affirmer le principe de légalité en matière de vidéosurveillance, c'est affirmer que la première légitimité d'un système de vidéosurveillance doit être fondée sur les législations en vigueur.

Ces législations traduisent un état d'esprit et révèlent des choix de société. Elles sont aussi révélatrices d'une culture, d'une histoire et de rapports de force, d'équilibres ou de compromis entre autorités/citoyens, villes/Etat ou encore entre les différents échelons territoriaux.

Elles mettent à jour des relations de confiance ou de méfiance et sont, par essence, un outil de légitimation d'une pratique.

C'est donc une base de travail essentielle.
Le premier échelon auquel les partenaires se sont intéressés est le niveau communautaire. Ces législations définissent des règles qui ont vocation à s'exercer dans tous les pays de l'Union.

>>

Ainsi, la charte rappelle que :

L'élaboration et le développement des systèmes de vidéosurveillance ne peuvent se faire que dans le respect de la loi et des réglementations en vigueur. Respect et conformité avec la loi européenne, nationale, régionale ou locale. Son développement doit également se faire dans le respect des normes en matière de protection des données, des textes en matière d'écoute de communications et de conversations, d'ingérences illicites dans la vie privée, de protection de la dignité, de l'image, du domicile et des autres lieux pour lesquels une protection analogue existe. Les normes concernant la protection des travailleurs doivent être également prises en compte.

Comment dès lors mettre en pratique ce principe de légalité ?

Cela passe par une connaissance des textes en vigueur. L'enjeu pour les partenaires était de mettre en exergue ces textes qui ne concernent pas spécifiquement la vidéosurveillance mais que les villes devront prendre en compte dans l'installation de leur système en plus de leur propre législation lorsqu'elle existe.

>>

➤ Les systèmes de vidéosurveillance doivent s'élaborer en cohérence avec :

1) Le droit européen et international :

➤ La convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (CEDH) du Conseil de l'Europe – 1950 ;

➤ La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – 1981 ;

➤ La charte des droits fondamentaux de l'Union européenne ;

➤ La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

2) Les réglementations nationales et locales régissant les systèmes de vidéosurveillance et la protection des données à caractère personnel ;

➤ Évaluer la pertinence d'une installation de vidéosurveillance au regard des objectifs pour lesquels la Constitution permet une limitation de l'exercice des droits fondamentaux des citoyens.

3) Les différentes jurisprudences existant en la matière

➤ Compte tenu des évolutions technologiques, en cas de vide juridique sur une question

spécifique, la mise en œuvre du système de vidéosurveillance doit veiller à obéir aux autres principes définis dans la présente charte.

A travers ce principe de légalité, il y a une affirmation : le respect des réglementations en vigueur est le premier acte de démocratie. Ces législations si différentes soient elles, permettent de cadrer le développement des systèmes de vidéosurveillance.
La prise en compte de la législation en vigueur est un gage de durabilité.
Ce principe de légalité donne un cadre de légitimation, d'objectivation de la vidéosurveillance, mais comme tout cadre, il doit être précisé.

La légalité mise en pratique

Ce principe de légalité se décline de manières différentes à travers l'Europe. Alors que dans certains Etats le fonctionnement de la vidéosurveillance est régi par une loi générale portant sur la protection des données, dans d'autres, comme la Belgique, l'Italie et l'Espagne, l'utilisation de cette technologie est strictement délimitée. Par exemple, la loi impose dans ces pays un paramétrage technique du système qui permette de masquer à l'image les zones privées (fenêtres et portes par exemple). La loi stipule également la durée de conservation des données personnelles et rend obligatoire d'informer le public sur l'identité de l'autorité responsable de l'installation et de la gestion du système. Sur ce dernier point autant le système italien que le belge impose le cadre à respecter lors de la communication envers les citoyens, en exigeant que toutes les villes utilisent le même panneau signalétique et fassent apparaître un certain nombre d'informations fixées par la loi.

Un autre aspect important du principe de légalité concerne la formation des opérateurs vidéo. Il est fondamental que ces personnels connaissent la législation en matière de protection des données. Celle-ci est obligatoire dans certains pays, comme par exemple le Royaume-Uni. Dans d'autres, comme la France, cette formation figure habituellement dans les prescriptions déontologiques données aux opérateurs par les autorités locales. Enfin, dans d'autres pays, la formation relève de la volonté des autorités locales.
Un troisième aspect fondamental du principe de légalité touche aux procédures de contrôle indépendantes des pouvoirs publics. De nombreux pays ont ainsi mis en place des entités indépendantes qui veillent au bon respect de la loi par les pouvoirs publics utilisateurs des systèmes de vidéosurveillance. Ce sont par exemple les comités éthiques en France, le « Garante de la Privacy » en Italie, ou l'Agence de protection des données espagnole (AEPD selon le sigle espagnol), qui dispose par exemple du droit de proposer des sanctions si les dispositions légales ne sont pas respectées.

L'utilisation de plus en plus répandue de la vidéosurveillance impose d'adapter les lois pour encadrer et limiter les ingérences dans la vie privée. Ainsi, au Royaume-Uni, un cadre stratégique national a été défini dès 2008 et le gouvernement élu en juin 2010 a inclus le thème de la protection de la vie privée face à la vidéosurveillance dans son programme d'action. Connaître et respecter la loi est évidemment une obligation sine qua non, mais rien n'empêche les villes de prendre des mesures allant au-delà de la loi afin de garantir le respect de la vie privée et des libertés fondamentales. Recueillir des expériences et formuler des recommandations à ce sujet étaient justement l'un des objectifs du projet qui a donné naissance à cette charte.

La loi n'est pas prescriptive ; elle donne un cadre qui permet de mettre en œuvre le système. Dès lors, quels éléments d'un système de vidéosurveillance peut-on considérer comme prescriptifs ? En d'autres termes, comment appliquer les principes de la charte lorsqu'il s'agit de mettre en place et/ou gérer un tel système ?

2. Principe de nécessité
Tous les partenaires l'ont constaté : la vidéosurveillance n'est pas une solution en soi mais un outil parmi d'autres d'une stratégie globale de sécurité. Face à l'évolution technologique de la vidéosurveillance et le nombre croissant de villes qui y ont recours, il est important de rappeler qu'elle ne peut constituer une fin en soi. Elle doit être nécessaire.
Mais comment définir une telle nécessité sans verser dans l'apologie de la vidéosurveillance ? Comment définir un principe de nécessité sans pour autant préjuger de la liberté de chaque ville de définir ses propres choix stratégiques en matière de sécurité, avec ou sans vidéosurveillance ?

Et d'ailleurs, peut-on dire que la nécessité est, en soi, un principe fondamental ?
Il est toujours délicat de définir le choix d'installation d'un système de vidéosurveillance comme une nécessité. Car une réponse à la question de la nécessité demande des connaissances sur l'efficacité de la vidéosurveillance. Quelle est la contribution de la vidéosurveillance pour résoudre une problématique spécifique ? La vidéosurveillance apparaît-elle comme la réponse la plus adaptée à tel ou tel contexte ?

Il n'existe pas de réponse simple à ces questions, dont les partenaires de ce projet ont longuement discuté. Les évaluations scientifiques donnent des ré-

sultats mitigés, comme l'attestent par exemple les études conduites pour le Home Office britannique (Welsh and Farrington 2002, Gill and Sprigg 2005, Gill *et al* 2005). Tout d'abord, il convient de distinguer la finalité du système : s'agit-il de prévenir la criminalité ou bien de faciliter l'investigation a posteriori ? Quant aux effets escomptés, ils peuvent varier considérablement dans la durée et ils ne sont pas les mêmes pour tous les types de délit. La fonction de prévention suppose que le délinquant potentiel raisonne et agisse de façon rationnelle. Or on sait bien que de nombreux délits sont commis, justement, «sous le coup» de l'émotion. L'efficacité de la vidéosurveillance pour l'investigation n'est pas non plus assurée, pas plus que son rôle dans la réduction du sentiment d'insécurité.

Autant de considérations à prendre en compte lorsqu'on parle de nécessité. Il ne s'agit pas d'une nécessité en soi, mais plutôt d'une nécessité qui doit être formulée au terme d'un processus de diagnostic. C'est le raisonnement qui aboutit à la décision d'installation d'un système de vidéosurveillance qui en révèle la nécessité.

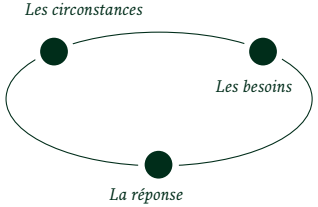
>>

DÉFINITION DU PRINCIPE DANS LA CHARTE :
L'installation d'un système de vidéosurveillance ne peut constituer en soi une exigence.
Elle doit se décider à l'aune d'une nécessité. La nécessité renvoie à l'adéquation entre des circonstances et un besoin d'une part, et la réponse que constitue le système de vidéosurveillance d'autre part. C'est ce besoin et ces circonstances qui rendent pertinente la décision, rende l'action inéluctable. Le principe de nécessité impose de faire clairement

apparaître le raisonnement derrière une action et qui la justifie. C'est ce principe de nécessité qui sous-tend la décision d'installation d'un système de vidéosurveillance. La nécessité a ainsi une dimension prescriptive. « Nécessité fait loi ».

Comment dès lors mettre en œuvre ce principe de nécessité ? A travers ce principe c'est la mise en avant du raisonnement qui justifie l'installation du système de vidéosurveillance. Ce raisonnement se structure autour de l'identification des circonstances, de la définition des besoins et de la nécessité de la réponse de vidéosurveillance.

Trois éléments sont constitutifs de ce principe de nécessité :



La conjonction entre les circonstances et le besoin fonde la nécessité de la réponse.

Ici, la charte reprend une méthode de résolution de problèmes similaire à celle qu'a utilisé la police britannique dans son travail de proximité (neighborhood policing). La méthode suivie ici est celle du procédé dit « SARA » qui signifie, selon le sigle en anglais, *scanning* (passer en revue un problème, une situation, des circonstances), *analysis* (analyser les besoins), *response* (définir une réponse) et *assessment*

(évaluer la réponse apportée au problème).
Le principal intérêt de cette approche est qu'elle permet de distinguer le problème à traiter des symptômes observés. Si l'on ne réalise pas les deux premières phases du *scanning* et de l'analyse avec suffisamment de rigueur, on risque d'aboutir à une réponse qui traite seulement les symptômes et non pas le véritable problème sous-jacent.
Dans le cas de la vidéosurveillance, le danger est qu'il est très tentant de croire qu'elle constitue la réponse recherchée et que dès lors, il n'est pas nécessaire de suivre tout ce processus. La question centrale n'est plus alors « quelle est la réponse la plus adéquate à ce problème ? » mais, « on souhaite installer un système de vidéosurveillance, comment peut-on le justifier ?».
Le principe de nécessité de la charte impose une approche différente, qui met le problème avant la solution, en considérant que, selon les cas, la vidéo peut être, ou non, efficace. Cette approche considère la vidéosurveillance comme une réponse parmi d'autres et elle permet aussi de relativiser son efficacité par rapport à d'autres outils de sécurité urbaine.

Il est très important aussi d'évaluer le système (la quatrième phase du processus SARA). Le principe de nécessité ne concerne pas seulement la décision d'installer un système, mais aussi chaque développement tout au long de sa « durée de vie ». La question de la nécessité est donc permanente. Elle se pose par exemple lorsqu'on envisage de l'élargir. S'agit-il d'un investissement nécessaire pour la sécurité[2] ? Elle se pose également si la situation de départ change. Par exemple, que faire lorsqu'on enregistre une amélioration significative de la sécurité ? La vidéosurveillance est-elle alors encore nécessaire ? Bien qu'il serait irresponsable de ne pas prendre en compte les investissements réalisés et que la question se pose de savoir quelles seraient les conséquences d'une suppression de la vidéosurveillance, il n'en reste pas moins que l'option de retirer les caméras est toujours envisageable.

[2] Evidement, le coût de l'élargissement d'un système est normalement beaucoup moins important, parce que l'investissement d'installation est déjà fait et et que les coûts fixes ne sont plus les mêmes.

Ainsi, la ville de Rotterdam a eu à un moment donné le projet de retirer certaines caméras, après avoir conduit un processus d'évaluation. Les habitants du quartier concerné s'y ont opposés parce qu'ils se sentaient rassurés par la présence des caméras. D'autres villes européennes ont eu la même expérience, ce qui révèle au passage que le principe d'implication des citoyens peut être plus complexe qu'on pourrait le croire. Dans le cas de Rotterdam, il a été décidé in fine de réduire le nombre de caméras, ce qui revient à donner une réponse adaptée à une nouvelle nécessité.

Un autre exemple intéressant est celui de la loi du Land allemand de Bade-Wurtemberg. Elle stipule qu'un système de vidéosurveillance peut seulement être considéré nécessaire s'il est statistiquement démontrable qu'une zone est particulièrement criminogène. A Mannheim, les autorités locales et la police ont dû démanteler un système de six caméras installé en centre-ville cinq ans environ après sa mise en place, parce que le taux de criminalité avait baissé de façon significative. Depuis le retrait des caméras, la situation est restée stable, ce qui pourrait aussi être lié à d'autres mesures prises par les autorités locales, comme par exemple l'aménagement de l'espace et de l'éclairage publics.

>>

RECOMMANDATIONS/ MODES D'ACTION

Dans ce contexte on peut recommander pour l'application du principe de la nécessité

Au niveau des CIRCONSTANCES

➤ Identifier de manière précise à travers un audit ou un diagnostic les problématiques de sécurité et de prévention de la délinquance repérées sur le territoire de la ville ;

➤ Dresser l'état des lieux des ressources locales disponibles et des dispositifs existants permettant répondre à cette situation de diagnostic ;

Au niveau des BESOINS

➤ Dégager les besoins issus du diagnostic et de l'Etat des lieux des potentialités locales. Les besoins doivent être précisés autant que possible car d'eux découleront les futurs objectifs du projet ;

➤ Considérer si d'autres moyens moins intrusifs sont possibles pour répondre à ces problématiques ;

Au niveau de la RÉPONSE

➤ Il faut définir les objectifs et identifier les bénéfices et les résultats attendus du système. Ces objectifs doivent être traduits en modes de fonctionnement. Il faudra ainsi définir par exemple quelles sont les implications fonctionnelles d'un système de vidéosurveillance qui fait de la prévention de la délinquance.

➤ Établir le type de système qui peut de manière réaliste permettre à la ville d'atteindre ces objectifs. Le système de vidéosurveillance doit être calibré pour répondre de manière pertinente et efficace aux besoins identifiés ;

➤ Les installations de vidéosurveillance ne peuvent être mises en service qu'à partir du moment où les autres mesures, moins intrusives, se sont révélées insuffisantes ou inapplicables (suite à une évaluation pondérée) ou que la nature du problème à résoudre soit hors de portée de ces moyens. En tout Etat de cause, la vidéosurveillance ne doit représenter qu'une partie d'une réponse coordonnée au problème identifié

➤ S'autoriser à appliquer un droit de retrait si nécessaire. Les villes doivent pouvoir considérer, sur la base d'une évaluation, que la vidéosurveillance ne relève plus d'une nécessité ou qu'il faudrait un redéploiement des caméras ;

Une fois la nécessité du système établie, reste encore à établir sa dimension et son calibrage par rapport au raisonnement mis pratique dans le cadre du principe de nécessité.

Ce calibrage des dispositifs de vidéosurveillance doit se faire dans la juste proportion.

3.Principe de proportionnalité

La proportionnalité est un principe qui a été difficile à définir. Elle peut être définie comme la juste mesure. Mais comment l'évaluer, à quel moment, par rapport à quoi ? De plus, comment peut-on déterminer la proportionnalité en dehors d'un contexte spécifique ? Comment prescrire dans une charte européenne ce qui est adéquat dans tel ou tel contexte spécifique à une ville ou une région donnée ?

L'important pour les partenaires, lorsqu'ils ont débattu de ce principe, n'était pas de définir une norme générale, mais plutôt d'insister sur la nécessité de calibrer le système de vidéosurveillance en fonction de chaque contexte particulier et des circonstances spécifiques.

Les comparaisons entre les systèmes de vidéosurveillance se font souvent en fonction du nombre de caméras. Mais ce n'est pas nécessairement le meilleur critère car le nombre de caméras doit être en cohérence avec les besoins identifiés dans la ville. Derrière ce principe de proportionnalité, il y a la recherche d'une juste mesure. Le déploiement d'un système de vidéosurveillance doit se faire en cohérence avec le raisonnement préconisé dans le principe de nécessité. Ce principe de proportionnalité est aussi lié au principe de responsabilité. En effet, définir un système qui respecte la juste mesure est un acte de responsabilité des autorités.

>>

Ainsi :

L'élaboration, l'installation, le fonctionnement et le développement des systèmes de vidéosurveillance doivent respecter une juste mesure

Le déploiement des systèmes de vidéosurveillance doit être mesuré par rapport à la problématique à laquelle elle souhaite répondre. Cette recherche de proportionnalité est avant tout une question d'adéquation entre les objectifs poursuivis et les moyens mis en œuvre pour les atteindre. Le principe de proportionnalité est donc intimement lié à la notion d'équilibre. Cet équilibre impose que l'installation de la vidéosurveillance ne puisse constituer la seule réponse de sécurité et de prévention de la délinquance développée dans une ville.

Quelle mise en œuvre de ce principe de proportionnalité ? Ce principe s'exerce à différents niveaux dans la définition et le déploiement du système.

RECOMMANDATIONS/ MODES D'ACTION

La proportionnalité doit être évaluée à chaque phase et dans chaque modalité du traitement des données, notamment quand il faut définir :

La taille de l'installation et les capacités techniques des caméras

➤ L'organisation technique et humaine doit être adaptée aux stricts besoins. Cela impose d'utiliser une technologie qui permette de répondre aux objectifs assignés sans aller au-delà. L'utilisation d'un système de vidéosurveillance doit être bornée dans le temps et dans l'espace : à un moment et sur un territoire spécifique en réponse à un besoin défini. Assigner une nouvelle fonction au système de vidéosurveillance

impose une réflexion sur la nécessité (principe I).

➤ Cette installation technique devrait intégrer notamment un système d'occultation des zones privatives par le biais d'un masquage dynamique, car un système de surveillance d'espace public ne peut avoir comme « effet secondaire » la surveillance de l'espace privé. De même, le positionnement et l'orientation des caméras ainsi que leur type (fixe ou mobile) doivent être adaptés à ce besoin.

La protection des données

Les images capturées par la vidéosurveillance constituent des données à caractère personnel et ainsi elles doivent être protégées au même titre que toutes données personnelles.
Cela impose l'adhésion à des règles strictes, régissant l'enregistrement, la conservation, le partage et la suppression éventuelle des images. Il importe de s'assurer que l es objectifs sont en adéquation avec :

➤ la décision de stocker ou non les images ;

➤ la durée d'une éventuelle conservation des données qui doit de toute façon toujours être temporaire. La durée de conservation doit être limitée au strict nécessaire, bridée et définie par paramétrage dans le système ;

➤ la protection physique et technique des données personnelles.

Il est donc nécessaire de définir les protocoles de gestion des habilitations d'accès et de transmission des images. Il importe d'intégrer dans ces protocoles la démarche « Privacy by

design » qui suppose que la protection des données personnelles soit prise en compte très en amont, dès la conception même des équipements de vidéosurveillance.

➤ Les systèmes de vidéosurveillance doivent trouver leur équilibre et leur proportion dans une politique intégrée de sécurité et de prévention de la délinquance. Ils sont un outil d'une politique de sécurité globale et doivent donc être en cohérence avec les autres réponses mises en œuvre localement.

La proportionnalité mise en pratique...

La ville de Saint-Herblain a initié, en 1997, un audit de sécurité avant la mise en place du système. Celui-ci a été réalisé par un cabinet extérieur. En parallèle, la Commission Sécurité du Conseil communal de prévention de la délinquance (CCPD) était chargée de mener une réflexion sur les questions de sécurité dans la ville de Saint-Herblain. Elle a remis son rapport en 1998 au sénateur-maire, qui a décidé de la création de plusieurs groupes de travail sur les thématiques intégrant ces questions de sécurité. En 1999, la synthèse des groupes travail a été présentée au Conseil municipal. De plus, une enquête d'opinion sur la sécurité, réalisée au travers d'un panel représentatif, a révélé que ce thème constituait la première préoccupation des habitants de Saint-Herblain.

Fort de tous ces éléments de diagnostic, le maire a initié un débat au sein du Conseil municipal sur l'application des propositions du CCPD, parmi lesquelles figurait la vidéosurveillance. En juin 1999, le Conseil municipal a voté l'installation d'un système sur la commune et la création d'un Comité d'éthique pour accompagner la mise en œuvre de ce projet.

On voit ainsi qu'à Saint-Herblain, le débat sur la vidéosurveillance est intégré dans une réflexion globale sur les questions de sécurité. Le diagnostic initial a permis de dégager un besoin et de donner des éléments de calibrage du dispositif.
La proportionnalité s'exerce à la fois dans la définition de l'envergure du système de vidéosurveillance mais aussi dans son intégration dans une politique locale de sécurité et de prévention de la délinquance. La vidéosurveillance est intégrée à une politique globale et elle est en cohérence proportionnellement aux autres éléments du dispositif.

C'est parce que l'installation du système répond à une nécessité et que son déploiement se fait dans une juste mesure qu'il sera transparent.

4. Principe de transparence
Durant tout le projet, une des questions essentielles des partenaires était : comment rendre lisible les systèmes de vidéosurveillance pour les citoyens et garantir le respect de leur vie privée et de leurs droits fondamentaux ?
La transparence est liée à l'information que l'on donne aux citoyens : quelle est l'information pertinente ? Jusqu'où faut-il informer les citoyens ? Les citoyens veulent-ils être informés ? Si oui, sur quoi ?
L'enjeu de ce principe est moins d'affirmer la nécessité d'informer les citoyens que de définir la nature des informations à fournir et les conditions de cette information.

Toute autorité en charge d'un système de vidéosurveillance doit avoir une politique claire et lisible quant au fonctionnement de son système

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

La transparence est très liée à la communication. Ce qui est transparent est ce qui se voit de l'extérieur. Ce principe se base donc sur l'information que l'on délivre. Ce principe est essentiel car si la vidéosurveillance peut être considérée comme une technologie restrictive de libertés, elle doit s'accompagner d'une forte information du public. Toute information autour du dispositif, respectant les législations en vigueur, ira dans le sens de ce principe de transparence.

RECOMMANDATIONS/ MODES D'ACTION

➤ L'autorité à l'initiative de l'installation des caméras de vidéosurveillance doit informer clairement les citoyens :

➤ sur le projet d'installer un système de vidéosurveillance

➤ sur les objectifs de ces caméras ;

➤ sur les moyens qui seront engagés pour la mise en place du système

➤ sur les zones vidéosurveillées. A cet effet, il est nécessaire de recourir à une signalétique visible et reconnaissable avec un pictogramme ;

➤ sur l'identité, la fonction et les coordonnées des personnes à qui s'adresser pour toute demande d'information. Ces informations doivent figurer sur les panneaux de signalisation des zones vidéosurveillées ;

➤ sur les mesures spécifiques de protection

des images enregistrées. Les données créées avec un système de vidéosurveillance doivent être protégées avec un accès restrictif par le biais de mots de passe. Elles doivent uniquement être utilisées pour les fins prévues, par les personnes autorisées et conservées le temps nécessaire. Toute utilisation de ces images enregistrées doit être notifiée dans un registre tenu à jour à cet effet ;

➤ sur les autorités qui peuvent être destinataires de ces images enregistrées ;

➤ sur leurs droits quant aux images les concernant. Il s'agit notamment du :

Droit d'accès à son image dans le respect du droit des tiers. Ce droit peut être refusé dans les cas d'enquêtes judiciaires ou encore dans des cas de risques liés à la Sécurité et à la Défense nationale ;

Droit de vérification de la suppression des images le concernant lorsque la date limite de conservation des images est dépassée ;

Ces informations doivent être compréhensibles et exprimées dans un langage clair et intelligible

➤ L'autorité en charge du système devra informer les citoyens régulièrement sur ses résultats et l'atteinte des objectifs, en s'appuyant sur les relais de communication habituels. Cela implique une formulation claire des objectifs en amont et nécessiterait des évaluations du dispositif fondé sur des indicateurs préalablement définis.

➤ Il est fortement déconseillé de recourir à des caméras fictives. Cette fausse information est de nature à discréditer le système et à engager la responsabilité des gestionnaires ;

La transparence mise en pratique

Toutes les villes partenaires du projet ont mis en œuvre un système d'information des citoyens sur leur système de vidéosurveillance.

A Rotterdam, par exemple, chaque fois qu'une caméra est installée, tous les acteurs concernés sont invités à voir le centre de contrôle, y compris les citoyens. L'expérience a montré que la transparence est très appréciée et qu'elle donne de bons résultats : 80 % de la population interrogée lors d'un sondage ayant comme objectif d'évaluer les divers dispositifs de sécurité se sont déclarés favorables à l'utilisation des caméras, et seulement 1.2 % était contre, le restant n'ayant pas d'opinion. La difficulté apparaît lorsqu'un incident survient et qu'il n'y a pas d'image enregistrée : alors, les attentes des habitants sont plus importantes.

La ville de Lyon également a initié une action forte en faveur de la transparence à travers l'activité du collège d'éthique ainsi qu'avec la signalétique. En effet, le collège bénéficie d'une bonne visibilité car 30-40 % de la population le connaît. Il y a également une signalétique qui respecte le cadre réglementaire et permet d'informer au mieux les citoyens. Sur chaque site vidéosurveillé, la signalisation est très claire et visible. Ainsi, le public est informé qu'il peut adresser toute réclamation au collègue d'éthique. En outre, la charte éthique rédigée par la ville de Lyon, qui reprend les engagements de la ville en faveur de la protection des droits des citoyens, est disponible sur le site internet de la ville, en mairie d'arrondissement, en mairie centrale et dans toutes les associations membres du collège.

5. Principe de responsabilité

Le principe de responsabilité doit garantir que la responsabilité du système est dévolue à une autorité précise. Il implique que ces responsabilités sont claires et connues et que cette autorité assume les responsabilités pour le système.

Le droit de surveillance de l'espace public est réservé à des autorités qui doivent être déterminées de manière restrictive. Ces autorités sont responsables des systèmes installés en leur nom.

Les autorités en charge des systèmes de vidéosurveillance sont les garants d'une utilisation légale et respectant la vie privée et les libertés fondamentales de ces systèmes. Leur responsabilité pourra donc être engagée en cas de manquements ou de violations constatées. Les autorités administratives devant lesquelles cette responsabilité peut être mise en jeu doivent être clairement identifiées. Les entreprises privées qui possèdent et gèrent des systèmes de vidéosurveillance visionnant des espaces publics doivent adhérer aux mêmes normes que les autorités publiques.

On pourrait se demander ce que serait une responsabilité sans sanction. La vocation de la charte n'est pas d'en définir mais bien de donner des outils de mise en avant des autorités responsables et de mettre en avant des pratiques de villes qui obligent les opérateurs d'assumer la responsabilité.

L'élection des élus locaux au suffrage universel est le gage de légitimité et de responsabilité par excellence. L'élu doit prendre ses responsabilités devant les électeurs et risque, en cas de manquement, de ne pas être réélu. Il faut noter cependant que dans la plupart des cas, les élus ne sont pas directement responsables d'un système de vidéosurveillance, notamment quand celui-ci n'est pas exclusivement municipal. Dans ce cas, il est plus compliqué d'identifier les responsabilités. C'est pourquoi le principe de responsabilité nécessite le principe de transparence.

La responsabilité ne s'applique pas seulement à la décision d'installer un système de vidéosurveillance, au bon fonctionnent du système et au respect des autres principes. Il s'applique aussi aux différentes utilisations du système, qui doivent être en adéquation avec les objectifs qui lui ont été assignés. L'un des risques est le phénomène de « function creep », c'est-à-dire le « glissement » vers de nouvelles fonctions qui n'avaient pas été planifiées à l'origine et auxquelles on trouve de nouvelles justifications, ou qui sont rendues possibles grâce à l'évolution technologique. La logique ne doit pas s'inverser et aboutir à ce qu'un système soit utilisé pour quelque chose parce que c'est possible, non pas parce que c'est nécessaire (principe 1). Si de nouvelles missions sont attribuées au système, elles doivent être appliquées sous la responsabilité explicite de l'opérateur.

RECOMMANDATIONS/ MODES D'ACTION

C'est pourquoi la charte suggère les recommandations et modes d'actions suivants :

➤ Communiquer le contact de l'institution et du service responsables et leurs coordonnées.

Chaque signalétique indiquant la zone vidéosurveillée pourra notamment comporter ces informations ;

➤ Affirmer l'obligation de confidentialité qui incombe aux gestionnaires du système. Cette obligation pourra être affirmée dans le cadre de la définition d'un règlement intérieur interne ou d'un code de déontologie à l'adresse des gestionnaires du système. Leur responsabilité pourra être engagée en cas de manquements à cette obligation ;

➤ Recourir à des mesures de sécurité permettant de protéger l'accès à la salle de gestion du système mais aussi de protéger l'accès aux images stockées. Des mesures techniques de contrôles de ces accès doivent être mises en œuvre ;

➤ Faire connaître les modalités de saisine des autorités administratives chargées de sanctionner tout abus constaté ;

➤ Mettre en œuvre un mécanisme approprié à la diffusion des informations nécessaires à la compréhension publique de l'utilisation de la vidéosurveillance.

6. Principe de supervision indépendante

L'une des idées clé pour une utilisation démocratique de la vidéosurveillance est de mettre en place un système de contrôle indépendant des gestionnaires de la vidéosurveillance. Comme l'a résumé le professeur Richard de Mulder, de l'université de Rotterdam, dans l'intitulé de son intervention lors de la conférence finale du projet : « Surveiller les citoyens :

pas de problème. Mais qui surveille les surveillants ? » Les citoyens doivent être rassurés sur le fait que les gestionnaires de la vidéosurveillance respectent leurs droits. Il faut donc un contrôle pour garantir que les opérateurs du système respectent les règles et les autres principes de la charte.

La supervision indépendante ne doit pas nécessairement être effectuée par une autorité de contrôle disposant d'un pouvoir de sanction, à l'égal de l'autorité publique qui a réglementé la vidéosurveillance. Le concept de supervision indépendante est à la fois plus souple que celui de l'autorité de l'Etat, et plus contraignant aussi. ***Il reflète l'idée de poids et contrepoids (« check and balance ») comme les fédéralistes ont appelé ce principe, qui était déjà à la base de la notion de séparation des pouvoirs telle que définie par Montesquieu (trias politica).***

Il ne nécessite pas de hiérarchie mais est fondé sur l'idée que la responsabilité n'est pas portée par un seul acteur. L'utilisateur de la vidéosurveillance est observé dans ses actions (principe de transparence) et doit rendre compte de ses actions (principe de responsabilité). Cette supervision doit être exercée par un superviseur indépendant des autorités qui gèrent le système de vidéosurveillance.

Le professeur Richard de Mulder explique bien combien les nouvelles technologies et la vidéo elle-même donnent de nouveaux pouvoirs à ceux qui les utilisent, ce qui présente un risque inédit de déséquilibre des pouvoirs et du système de poids et contrepoids qui fonde la démocratie. La solution, selon lui, est d'instaurer un quatrième pouvoir (outre les pouvoirs exécutif, législatif et judiciaire), qui serait celui de contrôle/surveillance/supervision, donc d'installer la *tetras politica*. Il existe déjà des institutions exer-

çant ce « quatrième pouvoir », comme par exemple la figure de l'Ombudsman (médiateur), qui peuvent superviser le bon fonctionnement et, plus important encore, intervenir quand un système ne marche comme souhaité.[3] De Mulder souligne aussi qu'il est plus important de s'assurer qu'il existe une telle figure de contrôle indépendant, plutôt que de chercher à prévenir tout dysfonctionnement. Le superviseur peut, le cas échéant, intervenir et rectifier un dysfonctionnement. C'est dans ce sens que la supervision est indépendante.

>>

L'idée de la supervision va au-delà de l'idée de l'autorisation. La supervision doit être assurée dans la durée et devrait s'appliquer à l'ensemble des enjeux de la vidéosurveillance et à toutes les phases d'un projet de vidéosurveillance.

.

C'est pourquoi la supervision indépendante est définie comme :

« des freins et des contrepoids au fonctionnement des systèmes de vidéosurveillance mis en œuvre par un processus de contrôle indépendant ».

Tout contrôle suppose la définition de normes. Ce principe de supervision indépendant permet à travers ces normes d'harmoniser les pratiques dans le sens de la Charte. Ce processus de contrôle indépendant peut prendre différentes formes et intervenir à divers moments dans le développement des systèmes. Il a son rôle dans la conception d'un système pour par exemple insister que la solution proposée corresponde au problème ou s'il a ce pouvoir de donner le feu vert à la vidéosurveillance.

Il peut ensuite accompagner l'installation du système et ensuite veille au bon fonctionnement et à la bonne utilisation du système, à la protection des données, à la formation des opérateurs de caméra, en discutant le résultat de l'évaluation du système pour décider de son développement.

Le « superviseur indépendant » peut être une personnalité qualifiée ou un organe spécifique composé. En particulier, il est possible de confier ce rôle aux citoyens.

Il existe de très nombreuses modalités d'organisation de cette supervision indépendante. D'ailleurs, dans la grande majorité des cas, elle existe déjà, à des degrés variés. Il y a des autorités qui donnent l'autorisation d'installer un système de vidéosurveillance comme, en France, une commission départementale dépendante du gouvernement central. En Italie, l'autorité de protection des données, la « Garante privacy » joue un rôle important dans la vidéosurveillance, s'appuyant sur une législation détaillée, de même qu'en Espagne, en France et en Belgique.

Dans les villes, c'est le conseil municipal qui, traditionnellement, remplit le rôle de superviseur et il est plus ou moins impliqué dans la gestion de la vidéosurveillance. L'exemple du conseil municipal montre aussi ses limites car ce sont souvent les mêmes majorités qui décident et supervisent la vidéosurveillance. Si le maire n'est pas élu au suffrage universel et donc indépendant de la majorité au conseil municipal ou si l'opposition n'a pas de rôle dans cette supervision, celle-ci ne peut plus être considérée comme indépendante. De plus, il faudrait que ce superviseur puisse s'auto-saisir ou être saisi par l'extérieur.

Dans la multitude de poids et contrepoids en place, les partenaires du projet ont identifié deux pratiques particulièrement intéressantes, qui assurent de manière très différente la supervision. D'une part, un comité éthique (comme mis en place à Lyon ou au Havre en France), d'autre part la figure du « visiteur indépendant » telle qu'instaurée dans le comté du Sussex au Royaume-Uni.

Comité éthique (France)

Le comité éthique est une institution spécifiquement mise en place pour la supervision de la vidéosurveillance dans les villes françaises de Lyon et du Havre, qui a pour mission spécifique de veiller au respect des libertés. « Sa composition répond aux objectifs d'équilibre, d'indépendance et de pluralité. Il est composé d'élus répartis également entre la majorité et l'opposition, de personnalités qualifiées représentant le monde du droit, de l'économie et de l'éducation, 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 informe les citoyens sur les conditions de fonctionnement du système de vidéosurveillance et reçoit leurs doléances. » (Art 4.1 de la charte éthique de la vidéosurveillance des espaces publics de la ville de Lyon). La charte éthique, comme celle que la ville de Lyon s'est donnée ou celle que le projet propose, peut fonctionner comme référence de base pour le comité et régler son fonctionnement. Le comité veille au respect de l'application de la charte éthique. Pour cela il élabore chaque année un rapport sur les conditions de fonctionnement et l'impact du système. Dans ce cadre, il peut demander au maire de faire procéder à des études par des organismes indépendants, comme la ville de Lyon les entreprend à l'heure où nous mettons sous presse (juillet 2010), avec une évaluation globale (technique et sociologique) de son système de vidéosurveillance réalisée par la faculté d'urbanisme et de l'aménagement de l'université de Lyon (professeur Jaques Comby). Ensuite, le comité éthique formule des recommandations au maire.

Dans la pratique, les comités éthiques de Lyon et du Havre sont très peu sollicités par les citoyens, ce qui peut aussi être interprété comme la preuve de leur bon fonctionnement. Les citoyens savent qu'un superviseur indépendant veille au respect de la vie privée et veille au bon fonctionnement du système. De plus, il peut se saisir de toute question entrant dans son champ de compétences.

Visiteurs indépendants (Royaume-Uni)

Le partenariat « vidéosurveillance » du comté de Sussex, regroupant la police et les collectivités locales, a opté pour une autre forme de supervision. Les citoyens eux-mêmes sont invités à vérifier le bon fonctionnement du système et contrôler la conformité au Code d'usage. Pour cela un groupe de douze citoyens a été recruté suite à un appel à candidats, afin de réaliser des vérifications ponctuelles des locaux de surveillance de la police et garantir la conformité au Code d'usage. De plus les visiteurs indépendants peuvent assister aux réunions d'examen des autorités de police et aux rapports annuels.

Les vérifications peuvent s'effectuer à tout moment, de jour comme de nuit, sans avertissement préalable. La plupart du temps, les visites sont effectuées par deux personnes. Au début de leur mandat, ces citoyens reçoivent une formation sur le système et le Code d'usage pour qu'ils sachent ce qu'ils doivent

contrôler. S'ils détectent un problème ou si quelque chose les préoccupe, ils en font part à l'autorité de police et à la direction de la vidéosurveillance.
Contrairement au système de comités éthiques, ce dispositif s'applique principalement au fonctionnement de la vidéosurveillance. C'est pourquoi il est complété par le travail de l'autorité de police qui associe les élus locaux. Ceux-ci en effet travaillent avec la police sur l'ensemble de ses activités, mais aussi sur le planning, la gestion, l'évaluation et le développement du système de vidéosurveillance. Ce dispositif est particulièrement intéressant par sa simplicité, l'implication des citoyens (principe 7) et sa grande transparence (principe 4).

Ainsi, pour l'application de ce principe de supervision indépendante, on peut recommander que :
➤ cette autorité indépendante soit chargée de fournir, après étude des dossiers, les autorisations d'installation des systèmes de vidéosurveillance ;
➤ elle soit chargée de veiller à ce que la mise en œuvre et l'usage du système respectent les règles et les normes définies.

7. Principe de l'implication des citoyens
C'est sans doute le principe qui est le plus directement lié à la thématique de ce projet européen « Citoyens, villes et vidéosurveillance » : comment prendre en compte les droits et les libertés des individus et comment impliquer les citoyens dans l'élaboration et la réflexion sur la mise en œuvre d'un système local de vidéosurveillance.

Impliquer les citoyens n'est pas une démarche aisée. Jusqu'où aller dans la vie privée des citoyens pour garantir leur sécurité ? Comment impliquer les citoyens dans un système qui est censé garantir la

confidentialité des informations qui en sont issues ?

Tout doit être mis en œuvre pour favoriser une implication des citoyens à toutes les étapes de la vie d'un système de vidéosurveillance.

Le principe d'implication des citoyens consiste à donner une voix aux citoyens, à travers différentes formes de consultation, de participation, de délibération et de codécision. Toute nouvelle installation ou l'extension des systèmes de vidéosurveillance devra toujours envisager la participation active des citoyens résidant sur le territoire. Les groupes de discussion ou autres moyens de participation des citoyens doivent être prévus et accomplis à chaque fois que cela est possible. L'implication citoyenne accroît les chances de succès.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

RECOMMANDATIONS/ MODES D'ACTION

➤ Soutenir la participation des citoyens sur l'identification des besoins dans le cadre du diagnostic préalable par exemple à travers la réalisation d'enquêtes de victimation ;

➤ Favoriser une implication initiale des citoyens sur l'implantation des caméras quand elle répond à un besoin. Cela peut prendre la forme de marches exploratoires ;

➤ Rechercher l'acceptation par les citoyens des projets de sécurité globale. Il est recommandé d'organiser des réunions publiques d'information des citoyens permettant de recueillir leur adhésion aux projets de la municipalité ;

➤ Favoriser la participation des citoyens au contrôle et à l'évaluation du système via des questionnaires de satisfaction :

➤ Un processus encadré et formalisé donnant aux citoyens la possibilité de visiter la salle de contrôle et de gestion du système de vidéosurveillance. Ces visites doivent pouvoir être impromptues. Tout refus doit être motivé (par exemple pour raison d'enquête judiciaire en cours). Cette possibilité doit être encadrée de sorte à ne pas mettre en cause le droit des tiers

➤ Renforcer l'engagement des autorités locales à mettre en place un instrument qui permette de manière régulière la participation des citoyens. La création d'une structure locale chargée de veiller à la bonne utilisation du système devra inclure une participation citoyenne active dans la vie et le développement du système.

Le principe d'implication des citoyens dans la pratique

Pour les villes impliquées dans ce projet, ce principe était déjà une réalité, car le projet même d'installer un système de vidéosurveillance venait comme une réponse à une demande accrue de sécurité de la part des citoyens. C'est le cas de la municipalité d'Ibiza (Espagne) par exemple, qui, après avoir analysé les demandes des habitants, les dispositifs déjà en place et les résultats, a décidé d'installer cinq caméras dans des zones où aucun autre moyen ne s'était avéré efficace.

D'autres municipalités, comme celles de Gênes, Le Havre ou Saint-Herblain, ont organisé des débats publics avec les habitants ou des rencontres avec des associations de quartier afin de déterminer les besoins et les meilleures façons d'y répondre.

A Rotterdam, ce principe est intégré dans toutes les politiques de la ville, y compris les politiques de sécurité. Pour s'assurer que les politiques proposées par la municipalité répondent bien aux exigences des citoyens, la municipalité évalue chaque année ses dispositifs de sécurité, qui comprennent le système de vidéosurveillance. Le maire se réserve le droit de pouvoir installer et retirer des caméras en fonction des réactions du public et des résultats obtenus.

Ce principe ne s'applique pas seulement lorsqu'il s'agit de décider d'installer des caméras ou pour évaluer si la réponse fournie par les autorités a répondu aux demandes des habitants. Il s'intègre à toutes les étapes de la mise en place d'un instrument d'une politique de sécurité intégrée, à savoir dans le fonctionnement même du système de vidéosurveillance. C'est en consultant les habitants que les autorités peuvent choisir l'emplacement exact d'une caméra, afin de sécuriser un espace perçu comme potentiellement dangereux. Ce dialogue permanent renforce le sentiment de participation de chacun aux décisions politiques.

A Liège, il existe des journées « portes ouvertes » au cours desquelles les habitants peuvent effectuer des visites commentées des salles de contrôle.

Dans le Sussex, le système des « visiteurs extérieurs » a été plébiscité par la population.

Ce sont autant d'exemples d'initiatives prises par les autorités responsables pour associer les citoyens aux politiques de sécurité.

III. Vers un langage commun de la vidéosurveillance en Europe : proposition d'une signalétique commune

Comment avancer ensemble dans le sens de la création d'une langage commun en Europe en termes de sécurité et vidéosurveillance ? Ce fut également un

des fils conducteurs de ce projet, centré sur l'importance d'une communication transparente vis-à-vis des citoyens. Devant une mobilité accrue des personnes sur le territoire européen, la nécessité de créer des références communes et de traduire les politiques publiques dans un langage facile à comprendre par tous est apparue comme une évidence. D'où l'idée de proposer une signalétique commune pour les villes utilisant les caméras de vidéosurveillance. Cette proposition répond aussi directement à une demande formulée par des instances européennes : l'Assemblée Parlementaire du Conseil de l'Europe a appelé dans sa résolution 1604 de 2008 à la création d'une signalétique européenne, comme l'avait fait en 2004 le groupe de travail Article 29 sur la protection des données dans son Avis 4/2004 sur la vidéosurveillance.

Une première étude portant sur ce qui existe déjà a permis de mettre en évidence de très bons instruments de communication mais aussi des manques à combler. Dans certains pays, comme la Belgique ou l'Italie, le cadre législatif portant sur la signalétique est très précis, fournissant une structure figée pour tous les détails à mentionner, allant jusqu'à imposer un pictogramme standardisé. Dans d'autres, la loi prévoit que les citoyens doivent être informés du fait qu'ils se trouvent dans une zone vidéosurveillée, sans donner de consignes précises, et c'est à chaque autorité responsable de décider la forme dont cette communication va s'organiser. C'est plutôt dans ce cas de figure qu'on a pu trouver par exemple des signalétiques ne comportant aucun pictogramme, écrites dans la langue du pays seulement, donc impossible à déchiffrer par un touriste, sans information sur l'identité de l'autorité responsable.
Au vu des résultats de cette recherche, il a été décidé que les partenaires de ce projet réfléchiraient sur la

création d'une signalétique commune et sur un cahier des charges.
Le fruit de ces réflexions fut qu'une signalétique européenne devrait absolument :

➤ contenir à la fois du texte et de l'image, pour être compréhensible par toute personne ne parlant pas la langue locale ;

➤ le pictogramme devrait refléter l'actualité des évolutions technologiques. De plus en plus de caméras de type « dôme » sont utilisées dans les villes, et comme elles sont nouvelles, elles ne sont pas forcément repérées ni identifiées par les citadins. En proposant un pictogramme qui rappelle le dôme, le projet souhaite non seulement informer les citoyens sur l'utilisation de plus en plus fréquente de ce type de caméra, mais également les informer de l'existence de cette nouvelle technologie. La signalétique joue aussi un rôle pédagogique.

➤ Pour ce qui est du texte, tous les partenaires se sont accordés sur le fait que le mot «vidéo» doit apparaître, car il est commun à toutes les langues européennes.

➤ Un autre élément important consiste à faire apparaître le terme d' « espace public », car il est nécessaire de signaler que la politique publique de sécurité concerne bien l'espace public et non l'espace privé.

➤ Il est apparu également important d'affirmer quel est l'objectif assigné au système de vidéosurveillance, pour que les habitants comprennent clairement le lien entre cet instrument et la politique locale de sécurité.

➤ Les règles de transparence des politiques publi-

ques exigent que l'autorité responsable de l'installation et du fonctionnement des caméras soit clairement indiquée, et qu'au moins un moyen de saisine directe soit prévu (téléphone, site internet).

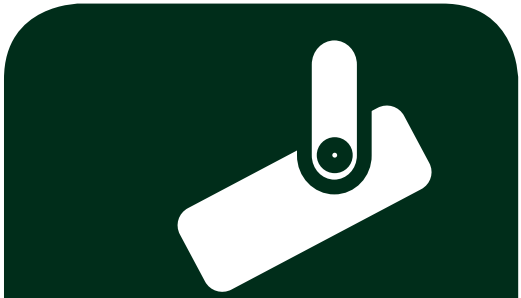
➤ Enfin, le principe de légalité selon lequel l'installation et la gestion d'un système de vidéosurveillance ne peut se faire que dans le respect de la loi doit aussi être inclus dans la signalétique, qui doit mentionner le cadre légal précis dans lequel le système s'inscrit et les dispositions concernant la protection des données.

Quelle utilisation pour cette signalétique ?
Dans la mesure où la plupart des villes ont déjà mis en place une signalétique, les partenaires du projet se sont évidemment demandé quelle serait la valeur ajoutée d'une telle signalétique pan-européenne.
En premier lieu, les recommandations de la charte pour une signalétique fournissant un maximum d'information peuvent inciter les villes à modifier et compléter la leur.
Pour les villes qui n'ont pas encore de signalétique propre, les recommandations peuvent fournir un guide facile à adapter au contexte local.
Pour d'autres autorités responsables du financement de la vidéosurveillance, comme les régions ou les ministères, les éléments cités ci-dessus peuvent constituer un cahier des charges pour le volet communication.
Last but not least, l'utilisation d'une signalétique commune à toute l'Europe contribuerait à une plus grande transparence des politiques publiques, bénéficiant à tous les citoyens des Etats-membres.


VIDÉO
SURVEILLANCE
POUR VOTRE
SÉCURITÉ
DIRECTIVE 95/46/CE
AUTORITÉ RESPONSABLE :
VILLE DE XXXX
PLUS D'INFORMATION
04 55 55 55 55
WWW.VIDEO-VOTREVILLE.FR
ESPACE
PUBLIC

Partie III

Zoom sur les villes : comment elles utilisent la vidéosurveillance et protègent les droits fondamentaux et les libertés



BOLOGNE

NOMBRE D'HABITANTS :
377 258

NOMBRE DE CAMÉRAS :
291

AUTORITÉ RESPONSABLE :
La ville

Ville de Bologne & Région Emilie-Romagne

Le projet de vidéosurveillance de la ville de Bologne naît de la volonté de trouver des solutions aux problèmes prioritaires : le sentiment d'insécurité, lié à la présence de groupes de dealers et la dégradation de certains espaces publics dans le centre historique de la ville.
Au mois d'avril 2000, le service responsable de la sécurité de la municipalité de Bologne a réalisé une enquête auprès de 753 habitants, afin de comprendre leur perception de l'insécurité. Les résultats ont démontré que le sentiment d'insécurité lié à la criminalité était particulièrement important dans le centre historique de la ville. Face à cette situation, l'admi-

nistration a décidé d'implanter un système de vidéosurveillance dans la zone nord-est du centre historique.
En juin 2000, ce projet préliminaire de vidéosurveillance est présenté par la ville de Bologne à la région Emilie-Romagne. En effet, la région finance régulièrement l'amélioration de la sécurité urbaine et des espaces publics dans les villes et en particulier la requalification urbaine, l'éclairage public et la surveillance des territoires à travers les nouvelles technologies.
Le projet de vidéosurveillance a été financé à hauteur de 50 % par la région Émilie-Romagne dans le cadre d'un accord de programme signé en 2002 avec la ville de Bologne.
Le coût total de l'installation a été de 1.829.164,80 euros. Le coût du réseau de fibre optique transmettant les images est d'environ 100.000 euros par an. Il faut y ajouter environ 50.000 euros de manutention par an.
De plus, environ 200.000 euros ont été débloqués en 2009 – financés à 66 % par la région Emilie-Romagne et pour le reste par la ville de Bologne – pour remplacer les caméras les plus obsolètes (installées en 2000), et pour améliorer les aspects technologiques de l'ensemble du système. Les coûts d'installation ont été partagés pour moitié entre la ville et la région. Les coûts d'opération et de manutention sont quant à eux intégralement à charge de la ville.
Au total 291 caméras ont été installées en ville. Le nouveau financement de la région Emilie-Romagne fera passer ce nombre à 315 d'ici à la fin de 2010.
Les caméras sont analogiques et dotées d'un système de vision nocturne. Dans 18 cas, il s'agit de caméras « dôme » (caméras orientables horizontalement à 360° avec possibilité de zoom).
Le système de transmission des données est coaxial et analogique. Le transfert entre les caméras et le

système d'enregistrement se fait par le biais d'un câble coaxial, tandis que les centrales opératives de police sont reliées par fibre optique. De futurs financements de la région Emilie-Romagne devraient permettre de relier l'ensemble du système par fibre optique.
Le « Projet Système réseau intégré de protection et sécurité » s'appuie sur l'implantation de technologies innovantes pour prévenir et limiter la délinquance.
Les images des caméras positionnées tout au long des parcours piétons les plus fréquentés et aux arrêts de bus, en centre ville, sont envoyées simultanément aux stations de la préfecture de police et à la station centrale de la police municipale. La préfecture de police peut ensuite les transmettre aux autorités judiciaires comme éléments de preuve. Les polices locale et nationale peuvent visionner les images cryptées et les conserver pendant sept jours avant leur destruction.

L'opérateur dans la station de la préfecture ou de la police municipale a la possibilité de visualiser les images de toutes les caméras et de diriger les caméras à distance.

La police municipale gère l'installation avec l'aide de techniciens d'une entreprise privée et l'aide de la police nationale. La police nationale, la police nunicipale et les carabinieri (gendarmes) contrôlent les caméras.

Dans la station centrale de vidéosurveillance de la police municipale, trois policiers travaillent simultanément par roulement permettant un contrôle 24h sur 24h.
Dans la station de vidéo surveillance de la préfecture de police, un inspecteur de la police d'Etat et deux

assistants sont présents 24h sur 24h. Un des deux assistants et l'inspecteur ont participé à la formation organisée par la ville de Bologne.

Le choix des opérateurs est limité par la législation nationale qui restreint le choix à des officiers de police judiciaire. Au total, les images sont consultées par une dizaine d'opérateurs répartis entre la police nationale, la police municipale et les carabinieri. Les images ne peuvent pas être transmises en temps réel à d'autres services.
Seuls des agents de police judiciaire peuvent accéder aux images enregistrées, sur autorisation des magistrats. Pour visionner les images, il faut non seulement une autorisation, mais aussi la clef d'accès physique. En revanche, seul le responsable de l'installation est habilité à consulter les enregistrements, et doit utiliser une clef d'accès spécifique.

La fonction de la police d'Etat est principalement répressive en temps réel (suite à l'alerte déclenchée par les images des caméras) mais elle permet également une forme de « pistage » des personnes suspectes par l'activation des zooms des caméras.

La fonction préventive est évidement liée à l'augmentation du risque pour les délinquants de commettre vols ou actes d'incivilités. Une plus grande surveillance du territoire permet de donner aux citoyens le sentiment d'une meilleure protection et d'une possibilité d'intervention plus rapide de la police.

Le réseau a été évalué avant, pendant et après son fonctionnement. L'évaluation s'est faite par le biais des statistiques des délits, des signalements de petits délits et d'incivilités, des dégradations urbaines et incivilités, et de la perception de l'insécurité.

Cependant il est difficile de mesurer la portée du projet de manière précise, car les statistiques de la criminalité ne sont pas assez détaillées (notamment d'un point de vue géographique) et ne permettent pas d'analyser correctement son évolution. Les forces de police s'estiment quant à elles satisfaites, car elles perçoivent la vidéosurveillance comme un outil efficace pour l'identification des individus et pour son usage devant la justice (donc l'aspect répressif). L'aspect préventif est moins clair. La satisfaction des citoyens est néanmoins importante, même si elle présente un recul par rapport aux expectatives exprimées avant la mise en place du réseau.
Les « displacement effects » (redistribution/délocalisation de la criminalité) ne sont pas quantifiables, par manque de statistiques fiables.

Gian Guido Nobili

➤ La vidéosurveillance à Brno a été mise en place par la municipalité et la police nationale dans le cadre des programmes de la prévention de la criminalité entre 1996 et 2008. Il s'agit d'un système de 18 caméras qui a nécessité un investissement d'un volume de 627.000 euros (considérant le taux de change en juillet 2010). Les caméras couvrent principalement le centre-ville, des espaces autour des gares et des arrêts de bus ainsi que les endroits très fréquentés. Avant l'installation du système la municipalité avait effectué une série d'études sur la sécurité à Brno, parmi lesquelles des enquêtes au sein de la population, des analyses sociodémographiques et des statistiques de police. Les travaux préparatoires ont également inclus des entretiens avec des policiers, des travailleurs sociaux,

des représentants des ONG et d'autres acteurs intervenant dans l'espace public.

Les principaux objectifs identifiés pour le système ont été :

➤ accroître le sentiment de sécurité dans les endroits de la ville avec les taux de criminalité les plus élevés ;

➤ prévenir la criminalité ;

➤ faciliter l'intervention des forces de sécurité en cas de délits dans les espaces vidéosurveillés.

En plus de ce système, 57 autres caméras sont installées dans différents districts de la ville et gérées par la police municipale et les autorités du quartier. Le coût de ce système était d'environ 2,3 millions d'euros environ (taux de change de juillet 2010). Ces caméras surveillent des endroits considérés comme problématiques, entre autre à cause de la présence de groupes de personnes dont on sait qu'elles sont souvent impliquées dans des affaires criminelles. De plus, l'entreprise de transports en commun de la ville utilise 24 systèmes à l'extérieur et a équipé 38 voitures de tramway avec des caméras. Enfin, le service d'entretien des routes utilise 64 autres caméras. Ni l'investissement, ni les coûts d'opération de ces systèmes ne sont publiés dans les rapports annuels de ces entreprises.

Selon la loi tchèque, seule la police nationale ou la police municipale peuvent gérer des systèmes de vidéosurveillance dans l'espace public. Les systèmes sont financés par le budget de la ville et des subventions de programmes pour la prévention de la criminalité. Le coût d'exploitation est pris en charge par les autorités de police et des entreprises de transport en commun et d'entretien de routes. Tous les systèmes de vidéosurveillance à Brno sont intégrés dans un réseau.

Selon la réglementation de l'Office pour la protection des données personnelles – qui a autorité pour sanctionner – des opérateurs privés peuvent être chargés de superviser certains espaces (semi-publics) comme des parkings, des supermarchés, mais leur système de vidéosurveillance ne peut pas enregistrer les images. Leurs images ne peuvent pas être utilisées dans des investigations de police.
Les enregistrements du système de vidéosurveillance de la ville de Brno et de la police nationale sont sauvegardés 20 jours et ensuite automatiquement effacés par des nouveaux enregistrements. Les images peuvent uniquement être vues par la police nationale (70 agents chargés de la surveillance et 3 membres du département des analyses). La police criminelle et la police routière peuvent également utiliser des images au cours des investigations. Les enregistrements sont gardés dans une salle spéciale au centre de commandement de la police nationale, auquel seuls des agents autorisés ont accès. Ces agents ont reçus une formation spéciale et eux seuls ont les codes d'accès à la salle.
La législation de la République tchèque en matière de protection de la vie privée est incluse dans le code civil et dans la loi sur la protection des données. Les autorités tchèques appliquent également le Code ISO des bonnes pratiques pour la gestion de la sécurité de l'information (CSN ISO 27 001). En outre, il existe un règlement spécifique au sein de la police pour la gestion des centres d'opérations et des directives pour le traitement de l'enregistrement vidéo de la police nationale. La fonction de contrôleur de la police pour la protection des données personnelle a été créée pour veiller à l'application de cette réglementation.

La technologie actuelle ne permet pas de flouter les espaces privés

Une carence qui doit être soulignée est le manque

d'information donnée au public. Les personnes ne sont informées de l'installation de nouvelles caméras qu'à travers des conférences de presse.
D'un autre côté, dans certains endroits problématiques, la ville a fait poser des panneaux dans les rues indiquant la présence de caméras, alors qu'il n'y en a en fait aucune. Cette initiative a été prise car cela a un effet dans la prévention de la délinquance et que cela augmente le sentiment de sécurité dans la population, à un coût très peu élevé.

La ville mène régulièrement des études parmi la population concernant leur sentiment de sécurité et leur appréciation du système de vidéosurveillance. Ces études indiquent que la majorité des habitants ne savent pas du tout où les caméras sont installées, mais estiment néanmoins être plus en sécurité grâce à la vidéosurveillance. En 2005, 4,5 % des personnes interrogées estimaient que l'installation de la vidéosurveillance restreignait leur liberté personnelle. En 2009, ce chiffre a baissé à 1,9 %. Etant donné la marge habituelle d'erreur dans ce type d'études, il est raisonnable d'affirmer que le nombre de personnes qui estiment que la vidéosurveillance empiète sur la liberté personnelle est maintenant négligeable.

De fait, le système de vidéosurveillance à Brno n'a pas engendré de quelconque débat public ou opposition. Il n'y a eu ni protestation publique, ni aucune initiative contre ou en faveur de la vidéosurveillance. Tous les partis politiques démocratiques représentés à l'Assemblée municipale de Brno incluent dans leur programme un chapitre sur la sécurité et la prévention de la criminalité. Et sur l'ensemble de l'échiquier politique, tous sont en faveur de la prévention. Toutes les phases de l'installation de la vidéosurveillance ont été discutées au Conseil sur la préven-

tion de la criminalité de la ville, puis recommandées au Conseil de la ville et enfin approuvées par l'Assemblée municipale de Brno. Au niveau national, le département de la prévention de la criminalité au ministère de l'Intérieur a été consulté et le projet a été approuvé par le Comité national pour la prévention de la criminalité.

Le public n'est pas autorisé à visionner les enregistrements vidéo, comme le dispose la législation. Dans le cas de crimes extrêmement graves, la police est autorisée à diffuser certaines images aux médias. Ceci est fait par le département d'information de la police, basé au siège régional de la Moravie du sud.

L'évaluation du système de vidéosurveillance est menée par le département de la prévention de la criminalité du ministère de l'Intérieur, entre autres grâce aux informations fournies par la ville et la police, y compris des analyses comparatives sur le taux de crimes et de délits dans les endroits vidéo-surveillés et dans ceux qui ne le sont pas. Il est intéressant de noter qu'effectivement, la vidéosurveillance a permis une diminution des crimes contre la propriété. Des groupes de pickpockets ont également quitté des endroits sous vidéosurveillance et migré vers d'autres zones moins « attractives ». En outre, des études montrent que les citoyens se sentent plus en sécurité dans des endroits surveillés.

Tous ces éléments montrent que le système de vidéosurveillance peut être considéré comme un outil utile dans le cadre de la politique de sécurité de la ville de Brno. Il peut être recommandé dans une société fonctionnelle et démocratique, à condition que les données et enregistrements soient suffisamment sécurisés par des moyens législatifs et techniques, garantissant les droits et libertés individuels fondamentaux. Le risque, comme toujours lorsque l'on manipule des données sensibles, est le facteur humain. Nous ne recommanderions certainement pas l'utilisation de la vidéosurveillance dans une société non démocratique où le chantage et l'extorsion sont courants.

Stanislas Jaburek

La vidéosurveillance en Italie et l'expérience menée par la municipalité de Gênes

➤ On assiste en Italie à une demande croissante des citoyens en matière de sécurité malgré la diminution, ou tout au moins la relative stabilisation du nombre de délits graves. Les facteurs qui contribuent à accroître cette exigence de sécurité sont essentiellement :

a) la médiatisation des délits et la recherche permanente du sensationnel, ce qui a pour conséquence de banaliser les crimes exceptionnellement spectaculaires et d'augmenter le sentiment général d'insécurité, sous l'effet d'un événement particulier ;

b) la peur de la diversité, un défi auquel nous sommes constamment confrontés en raison du rythme rapide et de l'évolution continuelle des changements sociaux et des problèmes liés à l'immigration ;

c) la conviction qu'on devrait trouver un moyen de contrôler tout aspect de notre cadre de vie, dans ses composantes individuelles ou collectives et que, par conséquent, tout événement négatif qui pourrait nous arriver devrait être imputable à la responsabilité de quelqu'un, tout au moins du point de vue de la responsabilité objective ;

d) le fait que « notre » comportement est une variable indépendante et qu'il appartient à quelqu'un d'autre de garantir notre sécurité.

Dans ce cadre, les mesures d'intervention les plus demandées sont :

1) des peines plus sévères ;

2) une police disposant de plus de ressources et de pouvoirs ;

3) des technologies de contrôle. Mais très souvent, ces dernières offrent des réponses en fonction des circonstances et seulement dans un nombre limité de cas.

En Italie, l'ordre et la sécurité publics sont du ressort de l'Etat. La récente modification de la législation a conféré aux maires des compétences en matière de sécurité urbaine qu'ils exercent par le biais d'ordonnances et, notamment, en développant des systèmes de vidéosurveillance.

Dans la ville de Gênes, les politiques municipales de sécurité urbaine ont commencé à se développer dans la seconde moitié des années 90, alors qu'émergeait une attente de plus en plus grande des habitants pour que la sécurité soit assurée non seulement par les institutions traditionnelles (forces de l'ordre et

autorité publique) mais aussi directement par les élus et les maires.
Ces politiques de sécurité se sont concentrées, dans un premier temps, sur une action dans le centre historique de la ville. Elles ont été menées dans le cadre du programme européen Urban II, qui a permis, avec l'accord de la préfecture de police, d'installer des caméras sous la responsabilité des forces de l'ordre, pour surveiller un certain nombre d'endroits sensibles. Suite au Pacte pour la sécurité conclu entre le ministère de l'Intérieur et l'Association nationale des communes italiennes, le pacte « Gênes ville sûre » a été signé en 2007 et c'est dans ce cadre qu'a été financé un projet de vidéosurveillance municipale. L'objectif principal était de mettre en place un outil de prévention de la délinquance afin de rassurer les habitants.

Afin d'identifier les points sensibles de la ville qu'il était opportun de vidéosurveiller, il a été estimé indispensable d'impliquer les municipalités, en tant que représentants de la population résidant dans les zones concernées. Convaincus que l'identification des lieux et les choix des technologies à adopter doivent apporter une réelle réponse aux besoins de sécurité des citoyens, nous avons entamé un repérage des endroits critiques grâce à un système de géoréférencement, qui nous a permis de décider où installer les caméras. L'information des citoyens sur les résultats se fera via divers canaux de communication.

Il existe actuellement sur le territoire de la commune de Gênes trois systèmes de vidéosurveillance. Le premier, visant à contrôler la fluidité du trafic routier, est composé de 38 appareils placés sur les principales artères. La police nationale, grâce à son poste de contrôle central, gère de son côté 97 caméras. Enfin, les 60 premières caméras du système de vidéosurveillance municipal ont été installées en 2009.

Les lignes directrices pour garantir un développement adéquat du système municipal sont contenues dans l'ordonnance du Garant pour la protection des données personnelles, promulguée en avril 2004, et qui énonce quatre grands principes généraux :
1-Légalité
2-Nécessité
3-Proportionnalité
4-Finalité

Dans le but de garantir le respect de ces principes, une commission technique spéciale a été créée. Elle est composée d'un représentant de la police locale, d'un représentant de la police nationale et d'un fonctionnaire expert en vidéosurveillance. Elle est chargée, en fonction des besoins exprimés par les citoyens, d'identifier les lieux qui devraient faire l'objet d'une vidéosurveillance.
D'un point de vue législatif, le traitement des images est en général assimilé au traitement des données personnelles. Etant donné la grande différence entre la nature des données personnelles contenues dans les images, par rapport aux supports papier ou informatique, il a été estimé nécessaire d'aligner les modalités de traitement des images sur les normes en vigueur en matière de protection de la vie privée, afin de garantir la protection et les droits des citoyens.
A cette fin, la commune de Gênes a élaboré un règlement, actuellement en voie d'adoption, qui :
➤ énonce les principes généraux que doit respecter l'administration communale dans les activités de vidéosurveillance ;
➤ énumère les objectifs sur la base desquels l'administration peut effectuer le traitement des images ;
➤ délimite les situations dans lesquelles il est possible de faire appel à ces mesures de vidéosurveillance ;

➤ identifie les outils qui peuvent être utilisés ;
➤ impose l'obligation de la traçabilité des accès aux données enregistrées ;
➤ définit les modes de communication avec les citoyens et fixe la période pendant laquelle les images peuvent être conservées, en fonction des différents buts et objectifs poursuivis ;
➤ reconnaît les droits des personnes filmées ainsi que de l'ensemble de la population et définit sous quelles formes ces droits peuvent être exercés.
Notamment, le droit d'accès aux images des personnes filmées doit être défini par rapport aux objectifs des acteurs publics en matière d'efficacité, d'efficience et d'économie. Il convient également de prendre en compte la protection de l'identité des tiers. De plus, on doit respecter le principe de réponse à une demande raisonnable, dans le respect de l'obligation d'impartialité et de bon fonctionnement de l'administration publique, telle que stipulée dans la Constitution italienne.

Etant donné l'importance des ressources humaines et financières nécessaires à la mise en œuvre des systèmes de vidéosurveillance, il est indispensable d'évaluer et de vérifier son efficacité. Un premier pas effectué dans ce sens par la commune de Gênes consiste à réaliser périodiquement des enquêtes de satisfaction auprès des habitants. Elles ont pour objet d'évaluer l'impact des interventions sur le sentiment de sécurité des citoyens. Plus largement, la ville est aussi en train de définir une série d'indicateurs qui permettront de mesurer l'impact de l'ensemble des initiatives prises dans le cadre de sa politique de sécurité urbaine.

Mariapia Verdona

➤ La mise en place en juillet 2009 d'un système de vidéosurveillance dans la ville d'Ibiza, la capitale de l'île baléare du même nom, fait partie d'une série de mesures prises par la municipalité pour réhabiliter les quartiers du centre historique, rongés par la marginalisation et la délinquance. Les différentes équipes municipales qui se sont succédé à la mairie depuis 1987 ont investi au total quelque 50 millions d'euros dans la rénovation des trois quartiers les plus « difficiles » de la vieille ville, Sa Penya, La Marina et Dalt Villa : aménagement de rues en zones piétonnes, création de nouveaux espaces culturels, amélioration des infrastructures…
En parallèle, la mairie a renforcé sa politique de prévention de la délinquance en augmentant les effectifs de

police de proximité dans ces quartiers et en initiant, en 2006, les démarches auprès du gouvernement régional pour obtenir l'autorisation d'installer des caméras vidéo. Le dossier de présentation du projet incluait des données statistiques sur la criminalité locale ainsi que des articles de presse consacrés à la délinquance dans la vieille ville. D'autre part, toutes les caractéristiques techniques des caméras ainsi que leur emplacement prévu étaient indiqués dans ce dossier.

Avec une population permanente de quelque 41.000 habitants, la ville d'Ibiza (Eivissa en langue catalane locale) accueille chaque année quelque 400.000 touristes. Vols, menu trafic de drogue, ivresse sur la voie publique… Le succès touristique d'Ibiza -l'un des sites les plus fréquentés de la Méditerranée et l'un des hauts lieux de la légendaire « movida » espagnole- a un impact direct sur la délinquance, notamment celle liée au menu trafic de drogue. Celle-ci est particulièrement importante dans la vieille ville d'Eivissa, point névralgique de la vie nocturne. Selon une information publiée en juin 2006 par le journal local *Diario de Ibiza*, le taux de criminalité enregistré dans les îles d'Ibiza et Formentera était alors deux fois supérieur à la moyenne espagnole (118 « délits et fautes » par habitant, contre 49,3 en moyenne en Espagne)*.

La mairie a sollicité l'autorisation d'installer un total de cinq caméras vidéo, dont quatre ont été mises en place en juillet 2009. Le coût de l'installation a été de 89.600 euros et la maintenance est financée par la municipalité.

Protection des données et respect de la vie privée

Le conseil municipal est responsable de la conservation des enregistrements, déléguée à la police municipale, ainsi que de son usage ou destruction. Une équipe de huit opérateurs vidéo fait fonctionner les caméras et a un accès direct aux images. Une fois celles-ci enregistrées, seuls trois officiers de police gradés sont autorisés à les visionner. Il n'y aucune autre transmission, en direct ou différé, des images. Cependant, il est arrivé que la police municipale remette certains enregistrements à la police nationale, dans le cadre de ses enquêtes.

Les enregistrements sont détruits au bout d'un délai maximum d'un mois, sauf s'ils sont utilisés dans le cas d'une enquête sur un délit grave ou lorsqu'une procédure judiciaire est en cours.

Lorsque des faits potentiellement délictueux sont enregistrés, les vidéos sont remises aux autorités judiciaires dans un délai de 62 heures maximum après enregistrement. Lorsqu'il s'agit d'actes pouvant constituer une « offense administrative » liée à la « sécurité civique » (aux termes de la loi espagnole), les enregistrements sont remis immédiatement aux autorités compétentes, afin d'initier une procédure pénale. En cas d'enregistrement illégal d'images et de sons, l'enregistrement doit être détruit immédiatement, conformément à la loi Fondamentale 4/1997.

Dans le cas où seule une destruction partielle de l'enregistrement est nécessaire et si la destruction totale est impossible ou inappropriée, pour des raisons techniques ou en fonction de la procédure utilisée, la personne responsable de la sauvegarde des enregistrements doit distorsionner ou bloquer les sons et images en question afin de les rendre inutilisables. Elle doit le faire selon les moyens techniques disponibles.

Information du public

Les habitants d'Eivissa ont été informés de l'installation du système de vidéosurveillance principalement via une campagne de presse dans les médias locaux. La population des quartiers concernés a également été informée par les autorités locales de toutes les dispositions de la loi sur la protection des données personnelles, et les procédures de recours en cas d'anomalie.

De plus, les habitants des immeubles où les caméras ont été installés ont été informés personnellement par les personnes en charge de l'installation, qui ont requis leur consentement (bien que ceci ne soit pas légalement obligatoire). En revanche, on peut noter qu'hormis les habitants des immeubles où les caméras ont été posées, le reste de la population d'Eivissa n'a pas été informé de l'emplacement exact des dispositifs.
La mise en place du système de vidéosurveillance n'a provoqué aucune contestation ni controverse. Tout au plus y a-t-il eu quelques protestations quant au délai de mise en place, jugé trop long par certains.

Un bilan positif
Au terme de la première année de fonctionnement, l'équipe municipale et la police locale jugent positives les retombées du système. Il a permis de réduire les actes de délinquance et a aussi servi dans le cadre de plusieurs opérations de police. La vidéosurveillance constitue ainsi un complément utile au travail de police de proximité effectué dans les quartiers de la vieille ville d'Eivissa. De façon générale, c'est aussi l'avis d'une majorité de la population locale.

** « Las Pitiüses duplican la tasa media de delincuencia por habitante de España », Diario de Ibiza, 6 juin 2006.*

Manuel Ayala Garcia

➤ Nous avons mis en place au Havre un partenariat permanent avec les services de l'Etat – le sous-préfet - , de la Justice – le procureur de la République, la police nationale – le chef de la Sécurité publique pour l'arrondissement du Havre, l'Education Nationale – l'inspecteur d'Académie, que nous réunissons systématiquement tous les 15 jours avec le premier adjoint au maire, l'adjoint chargé de la sécurité, et la direction de la sécurité municipale, dans le cadre de la cellule restreinte du Comité local de sécurité et de la prévention de la délinquance (C.L.S.P.D).

➤ Nous avons, dès les premières réflexions autour d'un projet d'installation de vidéosurveillance,

soumis cette question à nos partenaires pour avis, puis à chaque étape de la mise en œuvre, de la réalisation, de la création d'un éventuel comité d'éthique, de sa composition, et nous poursuivons ces échanges lorsqu'il apparaît nécessaire d'étendre les zones vidéo surveillées.

➤ C'est parfois à la demande de la police nationale que nous envisageons et proposons une extension en fonction du nombre de faits réels de délinquance, de façon durable, dans une zone ou un quartier.

➤ Ce n'est donc qu'après une réflexion collective, et toujours avec le temps utile, que nous mettons en place des caméras supplémentaires, et non en réagissant à la demande d'un concitoyen, victime d'un méfait.

Les demandes de caméras dans tous les quartiers, par des personnes privées, des commerçants ou des chefs d'entreprises sont si nombreuses d'ailleurs que nous ne pourrions répondre à toutes.
De 2004 à fin 2005, date de l'installation des trois premières caméras dans un centre commercial de quartier qui allait fermer en raison de la délinquance que nous ne parvenions pas à juguler, l'adjoint à la sécurité a informé le conseil municipal du projet et a reçu les représentants de tous les médias (presse écrite, radio, télévision), des associations (Ligue des droits de l'Homme, associations de quartiers) et tous les Havrais qui sollicitaient rendez-vous pour s'informer sur la démarche. Le maximum d'informations a été transmis, avant, pendant, et depuis l'installation. Information évidemment exacte, transparente et complète.

Nous considérons que la vidéosurveillance urbaine est un outil au service de la politique de sécurité et de prévention de la délinquance dans le cadre du contrat

local de sécurité de la ville du Havre. Ses objectifs sont de prévenir les atteintes aux personnes et aux biens, de participer au sentiment de sécurité des personnes et de sécuriser les bâtiments communaux et espaces publics exposés.

Cette action doit se concilier avec l'impératif de respect des libertés publiques et individuelles conformément à l'esprit de la loi d'orientation et de programmation de la sécurité du 21 janvier 1995 et de ses décrets d'application.

C'est dans ce souci permanent de garantir aux citoyens une exigence maximale de protection que la ville du Havre a souhaité la création du comité d'éthique de la vidéosurveillance des espaces publics.

Ce comité d'éthique est composé de trois collèges :
➤trois élus dont un désigné par l'opposition municipale.

➤ trois personnalités qualifiées :
• l'ex-Président de l'université
• un ancien bâtonnier des avocats
• un représentant de la Chambre de commerce

➤ trois représentants d'associations
• le président de l'association d'aide aux victimes
• le président du Conseil supérieur des Sénégalais du Havre
• le président d'une association de travailleurs sociaux

Le comité d'éthique de la vidéosurveillance des espaces publics est ainsi chargé :
➤ de veiller au respect permanent des libertés publiques ;

➤ d'informer les citoyens sur le fonctionnement du système ;
➤ d'examiner sur demande du maire du Havre toutes les demandes d'accès aux images et autres doléances des citoyens ;
➤ de formuler avis et recommandations au maire sur le fonctionnement du système ;
➤ de remettre au maire du Havre un rapport annuel sur le fonctionnement de la vidéosurveillance.

Toutes ces informations, et la réalité de son utilité, font que nous n'avons pas actuellement d'opposition, sinon marginalissime (!), au fonctionnement de la vidéo protection dans notre ville.

Bertrand Binctin

➤ Liège, ville millénaire, ville universitaire, métropole économique et culturelle de Wallonie, se situe au coeur d'une agglomération urbaine de 600.000 habitants, au carrefour de réseaux TGV et autoroutiers transeuropéens, à 100 km de Bruxelles, 25 km de Maestricht et 40 km d'Aix-la-Chapelle.

Cité ardente, de jour comme de nuit, elle privilégie la convivialité et l'hospitalité. Elle accueille de nombreux grands événements sportifs, festifs et culturels.

Dès 2002, le projet de rénovation du réseau de caméras de surveillance avait été inscrit parmi les pro-

positions d'actions prioritaires soumises au choix des citoyens liégeois, dans le cadre du chapitre « Une ville sûre » de la consultation citoyenne sur le projet de ville. Il avait été plébiscité à une large majorité des personnes ayant répondu à l'enquête.

Dès lors, à la demande du bourgmestre, les services de la zone de police locale de Liège ont installé un total de 109 caméras de surveillance, en plusieurs échelonnées sur cinq ans, de 2003 à 2008.

D'un point de vue technologique, il s'agit de caméras de type « speed dome » haute technologie, haute définition, qui permettent une rotation à 360° horizontalement et à 90° verticalement. Le zoom permet de lire clairement une plaque minéralogique à 150 mètres, de jour comme de nuit.

Ces caméras sont toutes paramétrisées de façon à rendre impossible la visualisation dans les habitations privées mais elles ne sont pas équipées d'un support intelligent pour l'exploitation des images. D'où l'importance de la formation des opérateurs, qui doivent aussi bien connaître le quartier qu'ils surveillent et sa population habituelle.

Les caméras sont reliées en réseau, par un un circuit fermé de fibres optiques – ce qui exclut tout risque de piratage. Les images sont visualisées au centre de gestion des événements ainsi que dans deux commissariats de quartier. Les données ne sont pas partagées avec d'autres services ou institutions.

La visualisation est effectuée exclusivement par des policiers – donc, par du personnel assermenté, tenu au secret professionnel.

Les images sont enregistrées et détruites après sept

jours, bien que la loi belge permette une conservation des images durant un mois.

Tout habitant peut solliciter la visualisation des images qui le concernent s'il en fait demande auprès du gestionnaire du système, c'est-à-dire le bourgmestre. Il est possible d'introduire un recours contre le gestionnaire du système.

Le Parquet et le juge d'instruction peuvent également solliciter des images dans le cadre d'une affaire pénale. Les lieux d'implantation des caméras ont été choisis en fonction des objectifs assignés au système, lors de sa mise en place. Il s'agit d'apporter une réponse de qualité aux trois types de problématiques suivantes :
➤ problématiques de circulation, par le visionnage des grands axes de pénétration dans la ville ;
➤ problématiques d'ordre public, par le visionnage des lieux de manifestations récurrentes ;
➤ problématiques de sécurité et d'environnement, par le visionnage de certaines zones sensibles, comme les artères des quartiers de vie nocturne.

Une signalétique spécifique est placée en affichage urbain : elle indique qui est le gestionnaire du système.
A chacune des quatre phases d'installation successives, les dossiers ont été soumis à l'approbation du conseil communal, où les craintes relatives au respect des libertés individuelles ont été publiquement débattues.

Les objectifs poursuivis ainsi que la localisation précise des caméras font régulièrement l'objet d'une médiatisation au travers de communiqués et de conférences de presse.

L'information à la population est également assurée via des contacts avec les comités de quartiers, une dé-

marche qui a été lancée avant même l'installation du système et qui se poursuit depuis par une évaluation régulière. Les participants à ces réunions sont ainsi ouvertement invités par le bourgmestre à exprimer leurs attentes.

En 2007, une commission de contrôle locale a été mise en place. Elle est composée de représentants de chacun des quatre groupes politiques démocratiques représentés au conseil communal de Liège et se réunit tous les deux à trois mois.

Elle a pour mission de garantir la bonne application de la loi de 2007.
En particulier, elle veille à ce que :
➤ la visualisation au centre «caméras» soit assurée exclusivement par du personnel policier spécialement formé ;
➤ la déclaration à la «commission vie privée» ait été correctement réalisée ;
➤ des paramètres masquent les zones particulières des immeubles privés ;
➤ des panneaux d'information correspondant aux prescriptions légales soient placés dans les rues concernées ;
➤ les images soient conservées, puis détruites après sept jours.

Les conseillers communaux sont régulièrement tenus informés d'éléments d'évaluation : résultats des travaux de la commission de contrôle locale, réunions de la commission spéciale de police, visites du «centre de gestion des événements»…

Le grand public est lui aussi convié régulièrement à visiter ce centre, par exemple dans le cadre des journées « portes ouvertes » de la police. Ces journées attirent un nombreux public.

En termes de coût, l'installation de l'ensemble du système représente un montant de plus de cinq millions d'euros. Les frais d'exploitation sont nuls, puisque le réseau repose sur la fibre optique. Le budget annuel de maintenance préventive est d'environ 100.000 euros. Il faut également compter avec les frais liés à la mise à jour régulière du système, notamment l'achat de nouveaux logiciels informatiques.

L'impact du système est estimé positif en termes de dissuasion et de sécurisation de la population ; cependant celui-ci n'a pas encore fait l'objet d'une évaluation externe.

Sur une période d'un an, les caméras ont permis d'établir 54 faits de criminalité en flagrant délit et d'apporter 58 résultats positifs à des demandes de suite d'enquête.

Catherine Schlitz

Description du projet de création d'un système de vidéosurveillance

L'expérience londonienne de la vidéosurveillance, en réalité l'expérience britannique, ne relève pas d'un projet unitaire. Tout d'abord, Londres est divisée en 33 zones administratives, chacune équipée de son propre système de vidéosurveillance. De plus, il existe de nombreux autres systèmes auxquels les autorités publiques ont accès, et il y a de nombreux systèmes privés de vidéosurveillance qui couvrent des espaces publics (des caméras appartenant à des entreprises, qui couvrent les points d'entrée et de sortie).

L'utilisation des caméras a augmenté de manière exponentielle au cours de ces dernières décennies. Au départ, des caméras furent introduites afin de contrôler la circulation dans les années 60. Plus tard des systèmes furent installés dans de grands centres commerciaux (dans les années 70 et 80), où il y avait une certaine ambiguïté par rapport à la nature de l'espace. En d'autres termes, dans les grands centres commerciaux, on a l'impression que les allées entre les magasins appartiennent à l'espace public, alors qu'il s'agit en réalité d'espaces privés. La plupart de ces centres commerciaux sont patrouillés par des agents de sécurité privés, en général selon un protocole avec la police locale qui leur permet / les encourage à faire des patrouilles régulières. De plus, la vidéosurveillance a été utilisée depuis un certain temps pour gérer les grands événements sportifs – notamment les matchs de foot, où elle s'est avérée un outil efficace de la stratégie pour supprimer la violence des stades et de leurs environs. A cela s'est rajouté une période prolongée de menace réelle de terrorisme, le tout permettant à la population britannique de se familiariser avec l'usage de la vidéosurveillance. Ce processus a été si abouti que très souvent ce sont les communautés elles-mêmes qui demandent l'installation de caméras.

Un facteur clef du développement de projets a été la volonté de réduire la criminalité, avec bien sûr l'objectif potentiel et supplémentaire de prévenir le terrorisme et de fournir une alternative précieuse aux détectives. L'utilisation de la vidéosurveillance est maintenant tellement omniprésente que nous avons tendance à supposer être observés, même si tel n'est pas le cas. La plupart (si ce n'est pas tous) des centres-villes à travers Londres sont sur-couverts par des caméras de surveillance. Il n'est pas facile d'affirmer avec précision combien de caméras il y a, cependant le Centre de commande et de contrôle de la

police peut avoir accès à plus de 60.000 caméras. A titre d'indication, l'aéroport de Heathrow comporte à lui seul 3.000 caméras.

Il a été soutenu, avec de plus en plus de détermination, que l'utilisation et l'emplacement des caméras se sont faits quelque peu au hasard. La tendance était de ne pas prendre en compte l'impact potentiel sur le déplacement des infractions ou des comportements délinquants et en outre, il y a peu de preuves de cas dans lesquels une fois le problème spécifique a été réduit, les caméras aient été enlevées ou redéployées. Ces problèmes sont maintenant traités de manière plus structurée grâce au développement d'une stratégie nationale pour la vidéosurveillance, sous la houlette du ministère de l'Intérieur (Home Office). Manifestement cette stratégie arrive longtemps après que l'usage d'une telle technologie soit bien établi. En effet nous sommes à la deuxième ou même troisième génération de caméras, puisque les autorités locales et leurs partenaires modernisent leurs systèmes pour profiter des évolutions récentes dans ce domaine.

Par exemple, il y a un changement de technologie de l'analogique vers le numérique, et une augmentation de l'utilisation des caméras dôme, qui comportent l'avantage que ceux qui sont dans la zone de vue ne peuvent pas savoir quelle direction la caméra balaye. Bien sûr, il arrive souvent qu'avec les technologies en vogue, l'envie de posséder le dernier matériel occulte la réflexion rationnelle qui décide quel niveau de complexité technologique correspondrait à une situation en particulier – une analogie facile serait d'acheter une Ferrari pour aller faire les courses au supermarché ! Il y a aujourd'hui une volonté croissante d'examiner les bénéfices accumulés par ce système, étant donné les coûts considérables qui sont

en jeu. Cependant il semble que le retrait des systèmes serait une décision politique difficile à prendre.

Avec l'émergence des systèmes de vidéosurveillance des autorités locales, à partir de 1985 environ, il y eu la présomption que ces systèmes devraient être sous le contrôle des autorités locales plutôt que de la police. Toutefois chaque projet d'installation avait toujours prévu que la police aurait accès aux caméras, que ce soit via des policiers présents dans les salles de contrôle ou par des images retransmises en direct aux salles de contrôle de la police, ou encore avec du personnel prêt à prendre le contrôle des caméras afin de surveiller des incidents spécifiques. Le développement rapide de partenariats efficaces entre la police et les autorités locales a contribué à l'effacement des limites nettes entre la police et les autorités locales en ce qui concerne le contrôle de la vidéosurveillance. Un certain nombre de salles de contrôle sont maintenant hébergées dans des salles de contrôle de la police, et bien que les opérateurs soient employés par des autorités locales, ils relayent constamment des informations à la police.

Un certain nombre de salles de contrôle gérées par des autorités locales ont la possibilité de mener des opérations confidentielles, ce qui permet de visionner juste quelques caméras bien particuliers sans que cela apparaisse sur le panneau commun d'écrans,à l'insu des opérateurs et sans leur participation. Le cas typique d'un exercice nécessitent la mise en place de cette option serait une opération anti-terroriste ou une opération d'envergure contre la criminalité organisée en direct. Ceci serait un moment clef à traiter par rapport aux questions des droits de l'homme et de la vie privée !

La législation dans ce domaine comprend la loi sur les droits de l'Homme (Human Rights Act) ainsi que la loi sur la protection des données (Data Protection Act). Il faut remarquer qu'il n'y a pas de clause légale spécifique pour la vidéosurveillance au Royaume Uni. Cependant la législation, y compris la loi de protection des données, s'applique à tous et n'est pas limitée aux institutions publiques. A côté de ça, comme nous l'avons signalé, la stratégie nationale pour la vidéosurveillance propose le développement d'une déontologie couvrant tous les aspects de la vidéosurveillance. De plus, le Royaume Uni, tout comme d'autres Etats, utilise des technologies diverses pour protéger les espaces privés de la surveillance indiscrète. Par exemple, les systèmes appartenant aux autorités locales ont souvent intégré la fonction de masquage dynamique des images qui concernent les espaces privés. Un exemple serait une propriété résidentielle au-dessus d'un commerce, dans une rue principale. Alors que la caméra parcours son périmètre d'observation, les zones privées sont automatiquement masquées. Toutefois il est possible d'annuler ce paramétrage (avec autorisation préalable) pour des situations qui l'exigent. De telles situations sont réduites aux crimes sérieux y compris le terrorisme, et nécessitent des autorisations de très haut niveau.

Tous les espaces couverts par la vidéosurveillance doivent comporter des panneaux qui indiquent la présence des caméras ainsi que des informations sur comment contacter les opérateurs. Cependant il semble que les caméras sont maintenant tellement omniprésentes qu'une telle signalisation est largement ignorée. Comme nous l'avons déjà noté, une stratégie nationale pour l'utilisation de la vidéosurveillance est en cours d'élaboration. Les documents relatifs à ces travaux sont accessibles sur le site Internet du ministère de l'Intérieur britannique (Home Office). Au moment de l'écriture de ce texte, le gouvernement de coalition récemment élu a indiqué ses intentions de renforcer la réglementation sur la vidéosurveillance. Ceci affectera la mise en pratique de la stratégie nationale, mais pour l'instant on ne connaît pas les détails de ce cadre législatif plus restrictif.

Il existe déjà des codes de conduite qui s'appliquent aux opérateurs surveillant les systèmes, ce qui forme la base de la formation qu'ils reçoivent. La plupart des salles de contrôle de vidéosurveillance sont elles-mêmes sujettes à des caméras de surveillance en permanence – un exemple de « surveillance des surveillants » ! En outre il existe la pratique de visiteurs externes qui peuvent inspecter les sales de contrôle de vidéosurveillance. Cette idée se fonde sur le même principe que celui qui fonctionne dans le cadre de l'accès aux personnes détenues dans les commissariats. Des volontaires de la communauté ont un droit d'accès direct à la zone de garde-à-vue et peuvent parler avec les prisonniers pour vérifier les conditions de leur détention. De la même manière, des volontaires peuvent se rendre dans les sales de contrôle des caméras, à l'improviste, afin de parler avec les opérateurs et s'assurer que les procédures requises sont bien suivies.

Il y a, dans tous les domaines concernant la prestation de services publics, une volonté d'impliquer plus les citoyens dans le processus décisionnel. Dans le contexte du maintien de l'ordre, cela se décline de plusieurs manières, par exemple avec des panels de citoyens. Cette initiative, qui fait partie du programme national pour la police de proximité réunit des individus parmi une communauté locale afin d'établir leurs priorités en matière de maintien de

l'ordre et de placer la police locale et ses partenaires devant leurs responsabilités face à ces priorités. Ces organisations peuvent agir en tant que catalyseur pour l'installation de systèmes de vidéosurveillance. La perception publique étant largement positive concernant les bénéfices potentiels de la vidéosurveillance, de tels groups deviennent de vrais militants pour des projets locaux. Ca peut même parfois engendrer la perception d'une police qui chercherait à atténuer l'enthousiasme pour la vidéosurveillance, en signalant que sa place est toujours comprise au sein d'un ensemble de mesures justifiées traitant d'un problème clairement défini.

Depuis quelques années, il y a une vague montante d'opinions favorables à la prudence (et non pas à l'opposition catégorique) face à la vidéosurveillance. Cette prudence semble venir autant des coûts par rapport aux bénéfices, que des atteintes à la vie privée. Il faut voir ce phénomène comme une conséquence des situations dans lesquelles des caméras furent déployées, sans considération des effets engendrés ou sans les ressources nécessaires pour répondre efficacement à ce qui a été observé ; rien ne diminue plus rapidement la valeur de la vidéosurveillance que la perception généralisée que personne ne viendra même si un délit se passe sous le regard des caméras.

Comme pour toute activité de sécurité de la communauté ou de maintien de l'ordre, la tâche d'évaluer l'efficacité de la vidéosurveillance est complexe. L'estimation de la performance face aux objectifs est difficile si les objectifs eux-mêmes sont déjà flous. Par exemple, efficacité signifie-t-elle prévention ou lutte ? Y a-t-il une valeur intrinsèque et mesurable du sentiment de sécurité apparemment induit par la vidéosurveillance ? Comment séparer les effets

de la vidéosurveillance de toutes les autres interventions qui ont pu être mises en place en réponse à un problème identifié ?
Selon certaines études empiriques, il semble que la vidéosurveillance peut réduire la criminalité et le désordre public, quoiqu'il soit moins certain que ces effets persistent forcément sur le long terme. Il existe également des preuves que la vidéosurveillance est efficace dans le contexte de crimes majeurs comme le terrorisme – même pour les attentats suicide – peut-être plus par rapport à la réduction des temps de reconnaissance nécessaires qui précèdent les attaques.

Il y a peut-être plus de preuves que la vidéosurveillance puisse fournir des renseignements précieux pour les investigations. Au minimum, elle fourni souvent des preuves irréfutables de conduite ou d'identification – il faut aussi noter que des études ont indiqué que l'existence de preuves par vidéosurveillance entraîne un pourcentage élevé de plaider coupable, ce qui évite le passage devant un tribunal et permet de réduire les coûts. Par ailleurs il a été démontré que lorsque des images de vidéosurveillance sont montrées, une sentence plus sévère est infligée.

En ce qui concerne la garantie, de nouveau les résultats sont mitigés. L'utilisation de la vidéosurveillance est tellement omniprésente que bien souvent elle est ignorée. En même temps, on pourrait se questionner sur sa tendance à augmenter la peur dans les zones non couvertes. Le besoin humain pour la sécurité est son propre moteur, qui demande toujours plus de garanties, que ce soit un policier à chaque coin de rue ou une caméra sur chaque lampadaire !
En conclusion, la vidéosurveillance est un outil précieux dans la boîte à outils de la sécurité urbaine,

mais ce n'est pas une réponse en soi ; elle doit s'inscrire dans une réponse stratégique planifiée, cohérente et bien documentée. Son efficacité doit être établie selon les objectifs assignés dès sa mise en application, au cas par cas. Les objectifs vont varier selon le type de criminalité et le territoire concerné et donc les preuves de succès vont varier en conséquence.

Andrew Bayes

Le collège d'éthique de la vidéosurveillance à Lyon

Dès que la ville de Lyon s'est orientée vers la mise en place d'un système de vidéosurveillance, il a été décidé de mettre en place une commission extra-municipale, baptisée collège d'éthique. Président naturel de cette commission, le maire de Lyon a délégué cette mission à une personnalité indépendante, le Conseiller d'Etat Jean-Pierre Hoss, qui a ainsi rempli ainsi le premier mandat du collège. Il a été remplacé, pour le deuxième mandat, par Daniel Chabanol, Conseiller d'Etat honoraire, ancien président de la cour administrative d'appel de Lyon.

La composition du collège a répondu à un souci de diversité : outre des élus de toutes tendances (opposition comprise), appartiennent ainsi au collège des membres de la société dite « civile », qu'il s'agisse de représentants d'associations, (telle la Ligue des droits de l'Homme,) ou de personnalités qualifiées (parmi lesquelles un bâtonnier honoraire de l'ordre des avocats et un recteur honoraire de l'académie de Lyon).

La mission officiellement confiée au collège s'articule autour de trois axes principaux :
➤ Rédiger un cahier des charges de la vidéosurveillance et le tenir à jour, notamment pour tenir compte des développements législatifs. L'objet de ce cahier des charges, proposé à la décision des élus, est, tout en respectant les prescriptions législatives, de définir des modalités complémentaires de capture et d'utilisation des images propres à accroître les garanties des utilisateurs de l'espace public. La réflexion actuellement menée (outre l'insertion des nouvelles normes législatives) est centrée sur les droits d'accès aux images et l'usage qui peut en être fait : les personnes filmées peuvent-elles obtenir le droit d'accéder aux images les concernant, et selon quelles modalités / quelles autorités peuvent-elles regarder les écrans « en temps réel », et à quelles fins / qui peut accéder aux enregistrements et à quelles conditions ?

➤ Recevoir les réclamations formées par des personnes ainsi filmées, donner un avis sur la suite à leur réserver, et faire toute proposition à cette fin. Il faut noter, et c'est normal, que cette activité est très marginale, rarissimes étant les réclamations sérieuses : par définition, les personnes qui seraient filmées dans des conditions discutables (par exemple en espace privé, en cas de dérèglement des

mécanismes qui s'y opposent), ou dont les images seraient conservées au-delà du temps légal, ou seraient vues par des personnes non habilitées ne savent pas qu'un manquement a été commis, et donc n'ont pas l'occasion de s'en plaindre…

➤ Constituer une base de données sur les pratiques en matière de vidéo-surveillance, observées tant en France que dans d'autres pays d'Europe. L'objectif est ici double. D'une part ces données devraient permettre de répondre aussi scientifiquement que possible à la question de l'utilité de la vidéosurveillance et l'on doit signaler que la ville de Lyon a lancé, sous le regard du collège d'éthique, une étude universitaire consacrée à cette question : un thésard s'engage dans cette recherche, dans un cadre universitaire strict (Universités de Lyon-II et de Genève), et bénéficie du soutien financier de la ville, toutes garanties étant données pour que cette recherche soit menée dans la plus totale indépendance universitaire.

D'autre part, les contacts noués à l'occasion du recueil de ces données devraient conduire à terme à la mise en place d'un réseau de municipalités, l'idée étant de conduire à une sorte d'essaimage de l'institution lyonnaise.

➤ Par-delà l'exercice de ces compétences, il est essentiel de noter que l'existence du collège, les échanges qui nourrissent ses réunions, ont pour effet, en dépassionnant un débat souvent fantasmatique, de conduire à une réflexion paisible et sereine sur un sujet sensible. Ce n'est certes pas à dire qu'un «consensus mou» prend la place d'un débat nécessaire sur un sujet de société fondamental. Ce ne serait pas souhaitable, et ce n'est pas le cas. Les oppositions sont présentes, et vigilantes, et la dialectique

entre les enthousiasmes des uns et les restrictions des autres est permanente. Mais elle enrichit la réflexion, plus que les exposés statiques de positions figées. C'est là l'apport essentiel de l'existence du collège.

Manuel Magne

La vidéosurveillance à Rotterdam : conserver un système efficace tout en gérant les attentes

La participation de Rotterdam au projet de l'Efus sur les caméras de surveillance est cohérente avec notre objectif d'améliorer notre système de vidéosurveillance. Quelles sont les options que nous n'utilisons pas encore ? Quel est l'équilibre entre la technologie et la capacité des individus à réagir aux événements ? Comment interpréter le concept de vie privée dans l'espace public ? Cet article examine notre expérience avec les caméras de surveillance à Rotterdam, les règles qui encadrent ce système et les problèmes particuliers sur lesquels Rotterdam travaille encore.

Expériences

Chaque ville essaye de contrôler la criminalité et les nuisances publiques. Chaque ville recherche des méthodes intelligentes et efficaces pour accroître la sécurité. Chaque ville peut utiliser les innovations technologiques. Rotterdam n'est pas une exception. La surveillance par caméra a pour but de réduire les nuisances publiques et la criminalité et d'augmenter le sentiment de sécurité de la population.

Les toutes premières caméras ont été installées à Rotterdam il y dix ans. La raison immédiate était le tournoi de football de l'Euro 2000. Il était important qu'il se déroule sans problème, ce qui signifiait être capable d'obtenir une vue d'ensemble précise de l'atmosphère et des événements au fur et à mesure qu'ils survenaient. Ainsi, des caméras ont été installées dans le centre-ville afin de surveiller les afflux en masse de supporters.
La même année, des caméras ont été installées à Saftlevenkwartier, un quartier près de la gare centrale. Pour ce projet-là, l'objectif était de réduire et prévenir les problèmes de violence et de harcèlement dans les rues.

Depuis 2000, le nombre de caméras dans les espaces publics a augmenté régulièrement jusqu'à atteindre 300. Il y a en outre un total de 1.600 caméras présentes dans le réseau de transport public (métro, trams, bus ainsi que gares et stations). Ces caméras appartiennent à des compagnies privées de transport, qui les contrôlent et les surveillent. Lorsqu'un incident se produit, elles peuvent transmettre les images en direct dans la salle de vidéosurveillance.
Chaque demande de caméra de surveillance est accompagnée d'un rapport détaillé qui décrit le nombre et le genre des incidents qui se produisent dans la zone et présente la situation locale en matière de sécurité. Toute décision d'installer une caméra est minutieusement examinée. On n'installe pas une caméra au hasard, mais parce qu'on est réellement convaincu que c'est un outil nécessaire pour améliorer la sécurité.

Les caméras de surveillance ne sont pas un remède contre tous les maux. A Rotterdam cependant, elles sont devenues un outil de base pour assurer la sécurité et prévenir les délits contre les propriétés et les violences.
Dans le cas des actes de violence par exemple, il est avéré qu'ils se produisent souvent « sur un coup de tête » ou sous l'influence de drogues ou d'alcool. La présence de caméras ne dissuadera probablement pas les délinquants, cependant elles peuvent tout de même être utiles : les images peuvent servir à fournir des preuves devant les tribunaux.

Les délits contre les propriétés tels que le pick-pocket ou les vols dans les voitures sont d'une autre nature : ils sont prémédités. Si des caméras ont été installées et que la police agit rapidement après l'infraction, le délinquant aura tendance à ne pas recommencer dans le même quartier. Ceci peut donc réduire le nombre d'incidents.

Conditions

Depuis l'arrivée de la vidéosurveillance, une même question revient régulièrement : comment l'utiliser de manière éthique et démocratique ? Plus il y a de caméras, plus il est important de gérer ces aspects correctement.

Aux termes de la loi hollandaise, ce sont les conseils municipaux qui autorisent la mise en place de caméras de surveillance. Si le conseil décide favorablement, il peut conférer au maire l'autorité de désigner

les emplacements où les caméras seront installées. Les décisions du maire sont rendues publiques et sont ouvertes aux objections des riverains. Une fois que les caméras commencent à enregistrer des images, celles-ci (et c'est toujours le cas à Rotterdam) dépendent de la loi sur les données de la police (Police Data Act), qui limite rigoureusement l'usage et l'échange de ces images.

Depuis le départ, la vidéosurveillance à Rotterdam est fondée sur un certain nombre de principes : toutes les caméras sont surveillées 24 heures sur 24, sept jours par semaine. Les images sont toujours enregistrées. Les riverains peuvent être assurés que tout incident sera remarqué.

Les incidents observés doivent être suivis. La présence de caméras signifie donc une intensification considérable de la surveillance dans un quartier. Non seulement parce que la zone est sous observation, mais aussi parce que chaque incident exige une réaction de la police ou des organismes de contrôle.

Quelques points à signaler

De nombreux partis politiques ont travaillé dur pour faire de Rotterdam une ville plus sûre. Nos habitants exigent que le gouvernement local garantisse une ville propre, correcte et sûre. Ils voient les problèmes dans leurs rues, sous leurs yeux, là où ils habitent. Il est donc vital que les conseils locaux répondent aux attentes des citoyens. Les caméras de surveillance sont un outil indispensable pour remplir cette tâche. L'investissement réalisé par Rotterdam est important. La vidéosurveillance est une technologie onéreuse et il faut également prévoir le financement de l'entretien des équipements et le coût en personnel, c'est-à-dire les équipes d'opérateurs ainsi que le personnel chargé des actions de suivi. A Rotterdam,

le nombre d'images qu'un individu peut surveiller simultanément est limité. Ce qui signifie que chaque fois que l'on installe une nouvelle caméra dans une zone, il faut recruter du personnel. C'est un point qui peut poser problème lors d'une nouvelle demande de caméra.

La valeur de la surveillance, cependant, est également importante. Des incidents qui n'auraient pas été remarqués autrement ou pour lesquels la charge de la preuve est complexe font maintenant l'objet d'enquêtes. En 2009, le département des caméras de surveillance a enregistré 23.700 incidents, soit 65 par jour. Nous devons continuer à estimer ces bénéfices par rapport aux coûts.

L'attitude des riverains a changé au cours des dix dernières années. Il y a dix ans, les premières caméras avaient été accueillies avec une certaine méfiance. Les gens avaient des doutes sur leur efficacité. De plus, ils n'avaient pas grande confiance dans le professionnalisme des utilisateurs et ils redoutaient les ingérences dans la vie privée.

Aujourd'hui, dix ans plus tard, les attitudes ont évolué de manière significative. En effet, les riverains se sont attachés à « leurs » caméras. De plus en plus, les gens demandent des caméras de surveillance dans leur quartier. Une enquête annuelle a également révélé un niveau très élevé de confiance envers le système de vidéosurveillance, que les riverains considèrent comme un outil efficace.

En conclusion

Les caméras sont devenues une caractéristique familière des lieux publics. A Rotterdam, elles ont prouvé leur valeur lors d'événements majeurs. Nous avons commencé à utiliser la vidéosurveillance à l'occasion

de l'Euro 2000. Récemment, elle a prouvé son importance lors de graves émeutes. En effet, grâce aux images des caméras, nous avons pu appréhender de nombreux émeutiers.

Notre expérience de la vidéosurveillance a donc été positive. Le cadre légal s'est développé pour répondre aux problèmes liés au droit civil et aux attentes du public en matière de sécurité. Nous avons mis en place une organisation et une structure de gestion solides. Les procédés opérationnels sont clairs. Nous devons poursuivre nos efforts pour maintenir ce système dans les années à venir. Cependant, il est clair que notre mission est amenée à changer, alors que de nouvelles questions surgissent et que de nouvelles attentes se font jour parmi le public. Nous devrons répondre à de nouvelles exigences. Dans le même temps, la crise économique entraîne d'importantes réductions budgétaires. Notre objectif est de contrôler le coût de la vidéosurveillance tout en maintenant notre budget. Un défi ambitieux qui demande une réflexion approfondie.

Afke Besselink, Niels Wittersholt

Saint-Herblain est une ville française de 45.000 habitants située dans la première couronne de l'agglomération nantaise (500.000 habitants). C'est la deuxième ville de l'agglomération nantaise et la troisième du département de la Loire Atlantique.

Le projet d'installation d'un système de vidéosurveillance a été initié par le sénateur-maire et les élus au début du mandat 1996-2002. Les premières caméras ont été installées à partir de 1999. La ville dispose aujourd'hui d'un système composé de 18 caméras. Elle a mis en place son Centre de supervision urbaine (CSU) en 2000 sur autorisation par arrêté

préfectoral. Ce centre avait initialement vocation à gérer uniquement le système de vidéosurveillance. Aujourd'hui, il permet de gérer simultanément la vidéosurveillance urbaine ainsi que le dispositif de télésurveillance et il tend à devenir de plus en plus un outil global de gestion urbaine.

En 1997, un audit de sécurité a été réalisé par un cabinet extérieur. Parallèlement, la Commission sécurité du Conseil communal de prévention de la délinquance (CCPD) était chargée de mener une réflexion sur les questions de sécurité dans la ville de Saint-Herblain. Cette commission a remis son rapport en 1998 au sénateur-maire qui a décidé alors de la création de plusieurs groupes de travail sur les thématiques liées à la sécurité. En 1999, la synthèse des groupes travail a été présentée au Conseil municipal. Parallèlement à ce travail au sein du CCPD, un questionnaire portant sur la sécurité a été administré à un panel d'Herblinois. Il a révélé que la sécurité était leur préoccupation numéro un.

Fort de ces éléments de diagnostic, le maire a initié un débat au sein du Conseil municipal sur l'application des propositions du CCPD, parmi lesquelles la vidéosurveillance. En juin 1999, le Conseil municipal a voté l'installation d'un système de vidéosurveillance sur la commune et la création d'un Comité d'éthique pour accompagner la mise en œuvre de ce projet.

La ville de Saint-Herblain a assigné trois grands objectifs à son dispositif de vidéosurveillance :

➤ sécuriser les lieux où les flux de biens et de personnes sont les plus importants en vue de réduire les délits sur la voie publique ;

➤ compléter par des moyens technologiques le dispositif de prévention de la délinquance existant (police municipale, actions de prévention en milieu scolaire) ;

➤ rassurer les habitants et fournir aux services de police d'Etat des éléments permettant l'élucidation des faits délictueux. L'objectif était double : accompagner la police nationale dans l'augmentation du taux d'élucidation alors très faible et sécuriser les espaces publics à vocation commerciale, industrielle ou de grands rassemblements.

Le système de vidéosurveillance a été mis en place pour améliorer la sécurité de tous les habitants de Saint-Herblain. Il est conçu comme un outil supplémentaire intégré à la politique locale de sécurité et de prévention de la délinquance. En ce sens, le Centre de supervision urbaine de la ville gère le système de vidéosurveillance et de télésurveillance, qui assure une plus grande réactivité des services municipaux (police municipale, services techniques etc.) et de la police nationale ou de la gendarmerie. Il s'agit donc d'un véritable outil de gestion de la ville.

La politique municipale en matière de prévention et de sécurité a été initiée il y a plus de vingt ans. Elle s'inscrit dans le souci permanent de prévention de la primo-délinquance et des conduites à risques, considérant que cette étape est fondamentale avant tout positionnement répressif. C'est au travers de différents outils -telles que les actions de prévention au sein des établissements scolaires, la prévention situationnelle, les interventions de la police municipale ou la réalisation d'actes réglementaires communaux pour ce qui concerne la gestion de l'espace public- que se traduit notamment la volonté politique de prévention.

L'ensemble des actions de prévention est organisé politiquement par l'adjoint au maire chargé de la pré-

vention et de la sécurité publique et administrativement au sein de la direction de la Prévention et de la tranquillité publique, qui est composée de 40 agents. Dans ce contexte, la vidéosurveillance urbaine constitue l'un des éléments de la politique globale de prévention et de sécurité. L'outil vidéosurveillance a été créé dans le strict respect des textes réglementaires régissant les libertés individuelles et notamment en ce qui concerne l'usage et le stockage des images. La ville a souhaité le faire en toute transparence vis-à-vis de la population. A ce titre, de nombreuses présentations et visites sont organisées permettant aux citoyens d'apprécier les garanties mises en place pour préserver la vie privée.

Le dispositif mis en place est composé de 18 caméras. Le CSU est composé de 14 agents et d'un responsable d'exploitation du système de vidéosurveillance. Un paramétrage numérique permet de respecter l'interdiction de visualiser le domaine privé ou de discerner les traits du visage d'un individu. En accord avec la réglementation en vigueur, des panneaux installés sur les différents accès routiers de la ville informent les citoyens de la présence de caméras.

Les images de vidéosurveillance de la ville sont transmises en temps réel au Centre d'information et de commandement de la police nationale.

Les images ne sont consultables que sur réquisition des services de la police nationale dans le cadre de plaintes déposées par des citoyens ou de demandes spécifiques des services de sécurité d'Etat.

Le système de vidéosurveillance a eu des effets positifs sur la sécurisation des espaces surveillés et la réduction des faits délictueux. En outre, aucun déplacement de la criminalité n'a été constaté.

L'activité du CSU (vidéosurveillance et télésurveillance) fait l'objet d'un bilan annuel. D'autre part, les opérateurs ont reçu une formation, réalisée par un organisme extérieur, sur les aspects déontologiques, l'environnement, le partenariat et les responsabilités dans le domaine de la sécurité.

Dominique Talledec

La naissance de la vidéosurveillance dans le Sussex

L'utilisation de la vidéosurveillance des espaces publics dans le comté du Sussex remonte à 1993, lors de l'installation d'un premier lot de quinze caméras dans les rues de Brighton, à la suite d'une décision de la police du Sussex et des autorités locales partenaires d'employer des caméras dans le but de lutter contre la délinquance et la criminalité. Cette première installation fut suivie par d'autres projets à Brighton et dans d'autres villes et villages – cofinancés par les autorités locales et des subventions gouvernementales. Dès le début, la vidéosurveillance s'est développée à travers une collaboration étroite entre la police et les autorités locales, avec la création de salles de surveillance dans les commissariats de Brighton, Haywards Heath, Bognor et Eastbourne, ainsi que dans les locaux de cinq autorités locales. Le principe de partage des coûts fut adopté en même temps.

Les initiatives gouvernementales en faveur de l'expansion de la vidéosurveillance continuèrent sous la forme d'une série d'appels à projet en 1994 (CCTV Challenge competition), et du Programme pour la Réduction de la Criminalité de 1999 à 2003. Cette dynamique reçut également une impulsion législative via la loi sur la prévention de la criminalité et des troubles à l'ordre public de 1998 (Crime and Disorder Act), qui obligea les autorités publiques à travailler ensemble pour s'attaquer aux problèmes de criminalité et de troubles à l'ordre public. En conséquence, en 2006, près de 30 villes et villages dans tout le comté de Sussex avaient déjà des caméras de surveillance, installés par 17 autorités locales et une association de bailleurs.

Ainsi fut créé le Partenariat Vidéosurveillance Sussex. Cette relation est aujourd'hui définie par des contrats légaux séparés entre la police du Sussex et chaque autorité locale, formulant les protocoles de fonctionnement, les rôles et responsabilités de chacun ainsi que les arrangements financiers.

La vidéosurveillance dans le Sussex aujourd'hui

Actuellement il y a plus de 400 caméras à travers le comté. Il s'agit d'un mélange de caméras analogiques Pan-Tilt-Zoom et de caméras dôme, reliées aux diverses salles de surveillance par un réseau de lignes de fibres optiques de transmission. La plateforme de contrôle, de surveillance et d'enregistrement est un système digital récemment installé qui

s'appelle « i-Witness » - conçu par Teleste et installé par BT Redcare. Cette plateforme permet l'enregistrement standard « de fond » de deux images par seconde, ainsi que l'enregistrement « en temps réel » de 25 images par seconde pour une séquence sélectionnée.

De plus, on a installé un terminal « client » dans chaque commissariat important et centre de détention, ce qui permet aux agents locaux d'avoir un accès instantané aux images s'ils ont besoin de faire des investigations.

Ce système complètement mis en réseau permet d'une part à n'importe quelle salle de surveillance du comté de visionner des images de toutes les caméras en direct et d'autre part permet l'accès immédiat de n'importe quel terminal client aux archives des enregistrements.

Bénéfices
Le fait d'avoir un système complètement mis en réseau nous donne un certain nombre de bénéfices opérationnels.

1. La continuité du service – le système est par nature résilient. Il est possible de faire fonctionner les caméras par n'importe lequel des nombreux points d'entrée du système, assurant ainsi au public la continuité du service.

2.Gain de temps pour les agents – les enquêteurs dans les commissariats peuvent accéder rapidement et facilement aux images dont ils ont besoin pour leurs enquêtes. La mise en réseau a permis d'éliminer le temps des trajets à travers le comté pour récupérer sur rendez-vous les images. La conséquence directe est que les policiers peuvent passer

plus de temps dans leur quartier pour assurer la tranquillité de leurs communautés.

3.Bénéfices environnementaux – réduction du nombre de trajets en voiture, donc réduction des émissions de carbone et des coûts de carburant.

4.Une justice plus rapide – les suspects arrêtés sont maintenant confrontés aux preuves vidéo à une phase avancée de l'enquête, ce qui entraîne une réduction du nombre de remises en liberté provisoires, des plaider coupable qui surviennent plus tôt dans la procédure, et pour finir un meilleur service pour les victimes.

5.La sécurité des images – l'accès est protégé par un mot de passe et est entièrement vérifié par un système de connexion d'activité qui garantit un meilleur contrôle des données confidentielles.

Les droits individuels, la vie privée et l'usage de la vidéosurveillance dans le Sussex
L'utilisation proprement dite de la vidéosurveillance dans le Royaume-Uni est régie par trois lois principales, ainsi que par des directives émises par le département britannique de la commission de l'information (Information Commissioners Office). La loi de protection des données de 1998 (Data Protection Act) établit huit principes de protections des données qui abordent le traitement juste et le contrôle convenable des données, l'exactitude de toutes les données retenues, et la proportionnalité des temps de préservation des données.

La loi sur les droits de l'Homme de 1998 (Human Rights Act) intègre dans la loi britannique les principes fondamentaux établis par la Convention européenne des droits de l'Homme – le droit au respect

de la vie privée de l'article 8 est particulièrement pertinent par rapport à la vidéosurveillance. La loi sur la réglementation des pouvoirs d'enquêtes de 2000 (Regulation of Investigatory Powers Act) instaure un règlement à suivre pour l'utilisation de caméras cachées, établissant des niveaux d'autorisation rigoureux.

Dans le Sussex, tous les opérateurs sont formés aux normes de l'Autorité de Sécurité (Security Industry Authority). Cette formation couvre les dispositions légales pertinentes, les responsabilités des opérateurs lorsqu'ils utilisent les caméras, et le respect pour l'égalité et la diversité. De plus, un Code d'utilisation de la vidéosurveillance a été adopté, qui établit les meilleures pratiques en termes d'utilisation fonctionnelle et éthique de la vidéosurveillance. Ce Code d'utilisation, que les partenaires partagent, auquel se rajoutent les protocoles entre la police et les autorités locales permet d'assurer l'uniformité et la compatibilité des systèmes.

Parallèlement, toute utilisation des terminaux clients situés au niveau local est garantie d'une certaine qualité à travers un programme de formation qui assure l'utilisation et la manipulation correctes des images vidéo confidentielles. L'existence de mots de passe individuels et d'un système d'accès approprié renforce encore ces garanties.

La confiance du public et la responsabilité de l'utilisation de la vidéosurveillance par la police dans le Sussex

Les autorités responsables de la vidéosurveillance dans le Sussex emploient principalement deux méthodes pour rendre compte de leurs actions devants les habitants: d'une part, des réunions de gestion rassemblant tous les partenaires de la vidéosurveillance et faisant l'objet d'évaluations rigoureuses, et d'autre part un processus innovateur de contrôle indépendant.

Gestion du partenariat

Le partenariat sur la vidéosurveillance du Sussex implique une approche partagée de la gestion et de la manipulation des caméras dans les espaces publics. Les caméras qui appartiennent aux autorités locales sont manipulées par le personnel de la police dans les commissariats et par le personnel des autorités locales dans les sales de surveillances des autorités locales, et les coûts d'entretien du système sont partagés.

Des réunions trimestrielles régulières entre la police de vidéosurveillance du Sussex et les autorités locales partenaires abordent les questions de performance du système, de développements techniques, de problèmes financiers et de défis à venir. L'utilisation par la police des caméras des autorités locales est ainsi justifiée.

Nous sommes en train de développer un processus pour mettre en œuvre l'installation de nouvelles caméras, afin de garantir l'uniformité des démarches dans tout le comté du Sussex.

Contrôle indépendant

Dans le Sussex, nous reconnaissons la nécessité de conserver la confiance du public dans l'utilisation de la vidéosurveillance. Un processus indépendant de contrôle et de vérification de l'utilisation des caméras par la police a été adopté. Les autorités de la police du Sussex ont recruté douze citoyens volontaires pour réaliser des visites de vérification ponctuelles des locaux de surveillance de la police, afin de garantir la conformité au Code d'utilisation. Celles-ci

peuvent s'effectuer à tout moment, de jour comme de nuit, sans avertissement préalable. Si les visiteurs détectent un problème ou un motif de préoccupation, la police et la direction responsable de la vidéosurveillance sont immédiatement alertées. La transparence est assurée à travers l'accès du public aux réunions d'évaluation des autorités de police et aux rapports annuels.

Aujourd'hui, on envisage d'étendre ce système de visites aux salles de contrôle gérées par les autorités locales partenaires.

Il est intéressant de voir que le travail effectué avec les partenaires européens dans le cadre du projet coordonné par l'Efus a confirmé la validité et la justesse de notre projet. Dans le Sussex nous considérons qu'un tel processus est un élément essentiel pour une future charte sur l'utilisation de la vidéosurveillance.

La stratégie nationale pour la vidéosurveillance et le Sussex

La stratégie nationale britannique pour la vidéosurveillance a été publiée pour la première fois en octobre 2007. Elle présente les résultats d'un large éventail de rapports concernant la vidéosurveillance en Angleterre et au Pays de Galles. Mise en chantier par une équipe formée de représentants de l'Association des chefs de la police (ACPO) et du ministère de l'Intérieur (Home Office), cette stratégie est maintenant soutenue par un comité multi-sectoriel, représentant un certain nombre d'acteurs.

Elle soutient et développe des recommandations afin de fournir :

1. une vidéosurveillance efficace et réussie, en prenant en compte le rôle de la technologie de vidéosurveillance et l'avis de la population ;

2.une meilleure pratique pour les partenariats entre les autorités locales, les opérateurs, les agents de police et les services d'urgence - pour offrir une meilleure protection aux habitants, autant comme moyen de dissuasion que comme une aide aux enquêtes policières ;

3.de meilleurs standards dans le fonctionnement de la vidéosurveillance et dans la présentation des images.

A travers les caractéristiques exposées ci-dessus, le partenariat de Sussex pour la vidéosurveillance cherche à adopter et à appliquer chacun de ces éléments essentiels, dans le but d'assurer la compatibilité avec les meilleures pratiques adoptées au niveau national.

Christopher Ambler, Roger Fox

La région Vénétie est située au nord-est de l'Italie et compte presque cinq millions d'habitants, dont 7 % issus de l'immigration, sur une superficie de 18.400 km^2. Elle est l'un des principaux pôles économiques et industriels italiens et figure parmi les 30 premières régions européennes. C'est également la région italienne qui accueille le plus grand nombre de touristes, avec un total de 60 millions de visiteurs par an. Elle est divisée en sept provinces et comprend 581 communes, dont 80 % ont moins de 5.000 habitants.

D'après les données générales concernant les phénomènes de criminalité dans la région, on a constaté au cours des dernières années une nette tendance à

la baisse, accompagnée toutefois d'un sentiment croissant d'insécurité. Ceci a incité plusieurs collectivités locales à mettre en place ou à développer des politiques de sécurité urbaine. Dès 2002, l'administration régionale a adopté un texte de loi (La Loi 9/2002) visant à soutenir et promouvoir un plan d'actions pour garantir la sécurité urbaine. La région souhaite créer un « système » destiné à gérer d'une façon coordonnée les problèmes complexes qui se posent sur son territoire, dans le cadre d'une collaboration entre les différents niveaux de gouvernement (Etat, région, provinces et communes) et les forces de police (nationale et locales).

Les communes et provinces ont ainsi été invitées à élaborer des projets intégrés de sécurité urbaine, qui ont ensuite été examinés et financés par la région. Lors des cinq dernières années (2005-2009), 278 projets ont été approuvés, financés et sont en cours d'exécution. D'après les données administratives, 131 comportent la mise en place de systèmes de vidéosurveillance (soit presque un projet sur deux).

En 2007, l'Observatoire régional de la sécurité (dont la création a été prévue par la loi régionale citée plus haut) a réalisé sa première enquête, afin de vérifier le nombre d'équipements de vidéosurveillance installés et d'évaluer leur utilisation. Sur l'ensemble des 581 communes, 215 ont répondu à l'enquête et les résultats ont permis de constater que la prise en charge du financement par la région a été l'une des raisons majeures qui ont encouragé la création et la mise en oeuvre de ces équipements. Par ailleurs, l'enquête a montré que la demande de vidéosurveillance a tendance à s'accroître.

Pour ce qui concerne les équipements choisis, dans plus de 70 % des cas il s'agit de systèmes numéri-

ques dotés de plus de trois caméras. Les lieux les plus fréquemment choisis pour l'installation des caméras sont les parkings publics, les carrefours, les parcs publics et les établissements scolaires. Dans environ 60 % des cas, on a assisté à une baisse des phénomènes de petite criminalité et de désordre public, d'après les estimations des commandants de la police locale ayant répondu au questionnaire. Il faut cependant souligner que dans 21 % des cas, on a observé que les comportements illicites se sont déplacés vers d'autres zones qui ne sont pas dotées de vidéosurveillance.

Un autre projet spécifique a concerné l'installation de caméras dans les moyens de transport publics des capitales provinciales de la région Vénétie. En effet, le système des transports publics urbains semble exposé à plusieurs facteurs de risque, tels que les actes de vandalisme, de violence et de petite criminalité, mais peut également être la cible d'attentats terroristes (comme l'ont montré les tragiques expériences de Londres et de Madrid). C'est pour cette raison que des systèmes de vidéosurveillance ont été installés dans le réseau des transports urbains, ainsi qu'aux arrêts de bus. Dans la ville de Venise, une attention particulière a été accordée aux embarcadères des « bateaux-bus » (les *vaporetti*).

La région a donc joué un rôle important dans la stimulation et la coordination des installations mises en place et gérées par les différentes collectivités locales ou par les départements. Cela a beaucoup contribué à développer l'utilisation et la diffusion de la vidéosurveillance dans les zones à forte concentration urbaine. Dans l'ensemble, le bilan semble plutôt positif, comme le montre l'augmentation exponentielle du nombre de systèmes mis en oeuvre.

Sur la base des activités et des expériences menées dans le cadre du projet européen sur la sécurité urbaine, il est maintenant important de s'interroger sur le rôle que peuvent jouer les administrations régionales dans la gestion des politiques de sécurité urbaine, notamment en matière de vidéosurveillance.

L'approche adoptée par la région Vénétie a depuis été imitée par d'autres régions italiennes. Deux éléments-clés de sa politique consistent d'une part à octroyer des aides économiques afin d'encourager les investissements des collectivités locales et d'autre part de proposer des instruments d'analyse afin d'identifier, au sein d'un projet local, les moyens les plus adéquats à mettre en œuvre pour aborder le thème de la sécurité urbaine. Etant entendu qu'il est préférable de traiter et résoudre les problèmes à l'échelon le plus proche de la population, c'est-à-dire au niveau local.

Il est toutefois possible d'envisager une deuxième phase, qui doit encore être développée, au cours de laquelle on pourrait prévoir que la région joue un rôle de coordination plus étroit vis-à-vis des communes, afin de garantir une plus grande homogénéité et une meilleure synergie dans l'application de leur politique de sécurité, pour ainsi éviter le risque d'isolement. D'autre part, on pourrait également encourager à l'échelle régionale l'utilisation d'outils complémentaires favorisant la participation et le contrôle. Ceci n'a pour le moment pas suscité beaucoup d'intérêt parmi les communes, qui se sont bornées jusqu'à présent à veiller à l'application stricte et bureaucratique des normes prévues par l'organisme national chargé de la protection de la vie privée.

En d'autres termes, il faudrait développer la coordination entre les collectivités territoriales du point de

vue des technologies utilisées, afin de permettre une plus grande efficacité des moyens de vidéosurveillance et d'obtenir des interventions immédiates et des actions préventives (grâce à l'utilisation d'autres banques de données disponibles et une meilleure organisation du service). En effet, ces systèmes ne sont utilisés pour le moment que comme un support technique d'appui aux enquêtes de police.

Les outils technologiques doivent cependant être soutenus par une bonne organisation des services de police. Dans ce sens, la région Vénétie est en train de réaliser un projet de répartition territoriale dans l'organisation des services de la police locale (la *distrettualizzazione*), qui permet d'associer plusieurs communes en agglomérations (« bassins de vie ») d'au moins 20.000 habitants, correspondant autant que possible à la structure de l'organisation de la police nationale. Ce nouveau découpage territorial permet aux plus petites communes de bénéficier d'un service de police municipale plus complet, en coordination avec la police nationale, qui garantit ainsi des interventions plus rapides et des actions préventives. C'est seulement par des activités de prévention, en effet, que l'impact de la vidéosurveillance peut être optimisé.

Parallèlement, il faut accroître l'implication des citoyens dans leur communauté et les sensibiliser davantage à l'utilité de la vidéosurveillance, qui, tout en étant assez invasive, est en général bien acceptée en Vénétie. Il est nécessaire que les citoyens soient convaincus des bienfaits de la surveillance civique et de la coopération afin de lutter contre les phénomènes assez répandus de dégradation et de désordre urbain. L'existence de « réseaux sociaux » civils est un fondement de la vie en commun, et c'est également une référence pour les forces de l'ordre.

Dans ce domaine, la région peut formuler des orientations réglementaires (élaboration de lois et de dispositions réglementaires appropriées), et agir sur le plan financier, en orientant les investissements vers vers une meilleure intégration des technologies selon des standards partagés. La région s'attache également à soutenir les administrations locales, en fournissant des lignes directrices et des directives, pour les aider à mettre en oeuvre des systèmes de sécurité urbaine comprenant l'installation de systèmes de vidéosurveillance dans une approche coordonnée en association avec les citoyens. Une telle démarche peut contribuer à faire évoluer le concept de sécurité et positionner la vidéoprotection comme un instrument parmi d'autres d'une politique globale.

Giorgio Vigo

Conclusion

Vers une utilisation de la vidéosurveillance respectueuse des libertés individuelles

En 2008, plus de 50 % de la population mondiale vivait dans les villes et la tendance va vers une augmentation de la mobilité entre les espaces urbains. Par conséquent, il y a une intensification des phénomènes urbains et cela se manifeste aussi en termes de sécurité. La vidéosurveillance, dans ce contexte, est, certes, un instrument technologique, mais elle illustre également une forme de collaboration sociale entre les différentes institutions et administrations.

La vidéosurveillance pose plusieurs défis que ce projet a eu pour objet d'approfondir :

1. Les rapports entre la vidéosurveillance, outil technologique, et le facteur humain qui la contrôle. Ce n'est pas la technologie en soi qui présente des risques, mais l'usage qui en est fait ; le risque que ses potentialités soient détournées doit être encadré dès l'installation des systèmes, à la fois par des mesures techniques et par un engagement politique.

2. Un système de vidéosurveillance peut être pensé comme un terminal intelligent, non seulement pour la récupération des images, mais aussi en termes de réorganisation des différentes ressources de la ville. Il peut faciliter le travail des agents de la ville ; mais cela demande des réponses moins génériques et plus adaptées aux besoins. Alors, la question de la sécurité pourra bénéficier d'une meilleure visibilité fondée sur une meilleure information des citoyens.

3. Le petit nombre d'études réalisé à ce jour sur l'efficacité de la vidéosurveillance a montré que les résultats obtenus grâce à cette technologie doivent être

mis en corrélation avec le contexte particulier dans lequel les caméras sont censées intervenir. Cela signifie prendre en compte la nature et la taille du territoire, la population mais aussi le besoin qui doit être identifié à travers des audits de sécurité. Experts et professionnels ont unanimement reconnu que la vidéosurveillance n'est pas la panacée qui pourrait régler toutes les questions de sécurité dans une ville, mais qu'elle doit être considérée comme un instrument parmi d'autres dans le cadre d'une politique globale de sécurité. Un équilibre est donc à trouver entre l'utilisation des différents outils que les décisionnaires ont à leur disposition. Il importe également de ne pas se limiter à l'utilisation d'un seul instrument car la véritable efficacité d'une politique de sécurité tient à la complémentarité des outils mis en oeuvre et à la capacité d'apporter des réponses coordonnées et adaptées à chaque situation.

4. La quête d'efficacité se traduit également par la possibilité d'intégrer différents systèmes de vidéosurveillance de l'espace public. Dans certaines villes, il existe effectivement plusieurs systèmes qui sont gérés par différents acteurs. Cette possibilité d'intégration des systèmes, qui suppose un meilleur partage de l'information, ne s'applique pas seulement au niveau local, mais aussi régional et métropolitain. Elle pourrait prendre la forme de pactes «transversaux» entre gouvernements, régions et municipalités ou, lorsque la législation le permet, de partenariats public-privé, en particulier lorsqu'il s'agit de surveiller des espaces semi-publics. Encore faut-il définir des protocoles précis et stricts de partage d'informations au vu du respect de la protection des données personnelles et de la vie privée. En même temps, le croisement de la vidéosurveillance avec d'autres systèmes d'information et bases de données, qui est en train de devenir techniquement possible, est à double tranchant. Bien que ceci augmente la capacité de surveillance des systèmes, le principe de la nécessité impose une justification rigoureuse du besoin d'accumuler et relier autant d'informations sur des individus.

Enfin, la question transversale déclinée à travers tous ces sujets a été de voir jusqu'où on peut aller pour assurer la sécurité des citoyens sans pour autant interférer avec leur vie privée. Existe-t-il un droit à l'intimité dans l'espace public ? Jusqu'à quel point ? Dans quelle mesure le droit à la sécurité peut-il affecter d'autres droits fondamentaux comme la liberté d'expression, d'association et de manifestation ?

Ces problématiques ont été abordées, à travers le prisme des habitants des villes, lors de ces 18 mois de coopération européenne. Les partenaires ont mis le citoyen au centre de leurs préoccupations. Les citoyens ont en effet besoin de se sentir en sécurité chez eux mais ils ne souhaitent pas pour autant que soit remis en cause leur droit à la protection de leur image. En tant que garants du bien-être des citoyens, les décideurs politiques se doivent donc de considérer cette question comme une préoccupation constante et mettre en balance ces différents aspects. D'un pays à l'autre, d'une ville à l'autre, la façon dont s'équilibre demande de sécurité et revendication d'un droit à l'anonymat varie. En examinant les politiques publiques au regard des perceptions du public, ce projet s'est donné pour but de renforcer la place et l'information des citoyens dans le cadre de l'utilisation des systèmes de vidéosurveillance, dans un souci de transparence indispensable à une mise en place démocratique des politiques publiques.

En tant qu'usagers ou acteurs des services publics, les citadins sont-ils ou non demandeurs de vidéo-

surveillance ? Celle-ci est-elle la réponse adaptée aux craintes exprimées ? Correspond-elle au budget disponible? Quelles formations et quels moyens de contrôle et de recours sont envisageables ?

Comment les citoyens expriment-ils leur demande ou refus de vidéosurveillance ? De quelle manière sont-ils informés et associés aux différentes étapes de mise en œuvre d'une politique de vidéosurveillance ? Comment ces dispositifs influent-ils sur les perceptions des citoyens et sur le comportement des victimes et auteurs potentiels ?

Autant de questions que les partenaires se sont posées et auxquelles ils ont essayé de fournir des réponses tant sous forme d'illustration de leur pratiques que sous forme de recommandations. Le résultat de ces interrogations et de cette recherche de solutions se traduit par la Charte pour une utilisation démocratique de la vidéosurveillance , un document qui atteste de la volonté politique des villes. Ces villes s'engagent à faire un usage de la vidéosurveillance qui respecte les droits fondamentaux des citoyens, et en toute transparence vis-à-vis du processus de prise de décisions.

C'est pour aller dans ce sens que les premiers signataires de la charte, le maire de Rotterdam (Pays-Bas), le président du Forum européen et maire de Matosinhos (Portugal) ainsi que le président du Forum français et maire de Saint-Herblain (France) invitent les autres maires à s'engager dans cette démarche volontariste.

Notes

Notes