Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 11478
04 janvier 2008

Vidéosurveillance des lieux publics

Rapport
Commission des questions juridiques et des droits de l'homme
Rapporteur: M. Yuri SHARANDIN, Fédération de Russie

Résumé

La vidéosurveillance est un phénomène de plus en plus répandu dans les lieux publics. L'évolution rapide des technologies et l'augmentation du sentiment d'insécurité dans la population ont contribué à faire accepter au fur et à mesure la vidéosurveillance comme un outil utile de prévention et de détection de la criminalité.

L'utilisation des nouvelles technologies est certes de plus en plus efficace en vue de garantir l'ordre public et la sécurité en Europe, mais on constate que la vidéosurveillance peut porter atteinte aux droits de l'homme.

Il convient d'apporter des garanties juridiques, procédurales et techniques afin d'assurer un recours à la vidéosurveillance en conformité avec les dispositions de la Convention européenne des Droits de l'Homme, telles qu'interprétées par la Cour européenne des Droits de l'Homme.

Le rapport expose l'existence de certains moyens techniques permettant de restreindre l'atteinte aux droits de la personne dans l'usage de la vidéosurveillance. Les Etats membres devraient systématiquement utiliser ces moyens.

Le rapport parvient également à la conclusion que les Etats membres devraient envisager l'adoption d'une signalétique uniformisée de la vidéosurveillance et préconise la poursuite des travaux du Conseil de l'Europe sur la question de la vidéosurveillance.

Sommaire **Page**

A. Projet de résolution

1. L'Assemblée parlementaire note que la vidéosurveillance est un phénomène de plus en plus répandu dans les lieux publics.

2. L'évolution rapide des technologies et l'augmentation du sentiment d'insécurité dans la population ont contribué à faire accepter au fur et à mesure la vidéosurveillance comme un outil utile de prévention et de détection de la criminalité.

3. L'Assemblée note que le recours à la vidéosurveillance en tant que tel n'est plus mis en cause. La technologie moderne permet de faire de la vidéosurveillance de haute qualité sans s'ingérer dans la vie privée des citoyens. Les craintes inspirées par le spectre de «Big Brother» semblent s'estomper.

4. Le fait est que, dans de nombreuses villes des Etats membres du Conseil de l'Europe, la vidéosurveillance s'est fondue dans le quotidien et a prouvé à plusieurs reprises son efficacité. L'Assemblée connaît le rôle positif qu'ont joué les systèmes de vidéosurveillance pour élucider des affaires pénales devant les tribunaux, par exemple dans le cas des attentats à la bombe perpétrés le 21 juillet 2005 dans le métro de Londres et, plus récemment, pour empêcher de nouveaux attentats à la voiture piégée à Londres et à Glasgow.

5. Tout en se félicitant de l'utilisation de plus en plus efficace des nouvelles technologies pour assurer l'ordre public et la sécurité en Europe, l'Assemblée demeure préoccupée par le fait que la vidéosurveillance puisse porter atteinte aux droits de l'homme, par exemple à la protection de la vie privée et des données. Eu égard notamment à l'article 8 de la Convention européenne des Droits de l'Homme (la Convention), qui garantit le droit au respect de la vie privée, la vidéosurveillance devrait rester une mesure exceptionnelle, encadrée par la loi et limitée aux cas où, dans une société démocratique, elle répond à un impératif de sécurité nationale et de sûreté publique, ou de prévention ou de détection des infractions pénales.

6. La collecte, le traitement et la conservation des données obtenues par vidéosurveillance doivent être régis par la loi, conformément à la Convention telle qu'interprétée par la Cour européenne des Droits de l'Homme.

7. A ce propos, l'Assemblée rappelle que plusieurs instruments juridiques, nationaux et européens, offrent des garanties minimales de protection des droits individuels au regard de la vidéosurveillance et que ces derniers devraient être respectés et pleinement mis en œuvre dans tous les Etats membres.

8. L'Assemblée est préoccupée par l'étendue des possibilités de surveillance permanente offertes au plan technique par les systèmes de vidéosurveillance. L'usage de ces moyens techniques devrait être strictement réglementé.

9. Etant donné que les équipements de vidéosurveillance et les logiciels existants permettent l'utilisation de zooms très puissants (facteur de grossissement jusqu'à 30x-50x) et d'une très haute résolution d'image, l'Assemblée encourage vivement les Etats membres du Conseil de l'Europe à adopter une législation limitant l'installation de ces équipements en fonction de la spécificité des lieux concernés.

10. L'Assemblée souligne aussi que les équipements de vidéosurveillance et les logiciels existants permettent de soustraire automatiquement à l'observation vidéo des «zones privées» (les fenêtres d'appartements, par exemple). L'Assemblée considère que cette pratique permet non seulement de protéger la vie privée des particuliers, mais aussi de préserver les employés de centres de vidéosurveillance de la vision de scènes qui ne relèvent pas de leur compétence. Dans les Etats membres du Conseil de l'Europe, il conviendrait de définir légalement ces «zones privées» et de faire en sorte que, grâce à l'utilisation de tels logiciels spécialisés, elles échappent à la vidéosurveillance.

11. Actuellement, les images des caméras de vidéosurveillance sont stockées au format numérique et il est possible de les protéger par chiffrement grâce aux logiciels informatiques, ce qui empêche la consultation des informations stockées par des tiers, les accès non autorisés et d'éventuelles modifications. Le chiffrement peut permettre que la validité des informations soit reconnue dans le cadre des enquêtes criminelles. Dans les Etats membres du Conseil de l'Europe, la pratique du chiffrement des données vidéo devrait être imposée par la loi.

12. Toute personne qui vit ou circule dans un espace sous vidéosurveillance a le droit de se savoir surveillée et d'obtenir l'accès à toute image d'elle-même. Les Etats membres du Conseil de l'Europe devraient protéger ce droit dans leur législation.

13. De plus, l'Assemblée souligne que la coopération entre organes gouvernementaux et entités non gouvernementales est capitale en matière de vidéosurveillance, et incite les Etats membres à intensifier cette coopération. Les gouvernements ont l'obligation de coopérer avec les ONG, lesquelles devraient avoir le droit de contrôler l'ampleur et la forme de la vidéosurveillance.

14. L'Assemblée note avec préoccupation que les lois nationales sont loin d'être homogènes en la matière et appelle donc formellement les Etats membres du Conseil de l'Europe:

14.1. à appliquer les Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance, adoptés en mai 2003 par le Comité européen de coopération juridique (CDCJ) du Conseil de l'Europe, et à veiller à ce qu'ils soient respectés de manière aussi systématique que possible;

14.2. à définir dans leur législation des restrictions techniques limitant l'installation de ces équipements en fonction du lieu surveillé;

14.3. à définir dans leur législation des zones privées à exclure du champ de la vidéosurveillance, en imposant l'utilisation de logiciels adaptés;

14.4. à prévoir dans la législation nationale la pratique du chiffrement des données vidéo;

14.5. à créer une voie de recours juridique en cas d'allégation d'utilisation abusive de la vidéosurveillance.

15. L'Assemblée 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.

16. Enfin, l'Assemblée – considérant qu'il faut approfondir la réflexion sur la vidéosurveillance – encourage la Commission européenne pour la démocratie par le droit (Commission de Venise) à se pencher plus avant sur cette question afin d'énoncer des principes conciliant l'intérêt public avec le respect des droits de l'homme et les libertés individuelles, propre à toute société démocratique.

17. Au vu de l'actualité et des progrès techniques constants en matière de vidéosurveillance, l'Assemblée souligne la nécessité de continuer les travaux sur le thème de la vidéosurveillance à l'avenir.

B. Projet de recommandation

1. L'Assemblée parlementaire se réfère à sa Résolution … (2008) sur la vidéosurveillance des lieux publics.

2. Compte tenu des travaux entrepris sous l'autorité du Comité des Ministres, notamment du Comité européen de coopération juridique (CDCJ), qui ont débouché sur l'élaboration des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance de 2003 – et convaincue que cette question mérite une analyse plus poussée –, l'Assemblée recommande au Comité des Ministres d'organiser une conférence sur la vidéosurveillance. Devraient y participer, entre autres, des spécialistes de la vidéosurveillance issus du secteur public et du secteur privé, ainsi que des représentants de la société civile.

C. Exposé des motifs, par M. Yuri Sharandin

1. Introduction

1. En septembre 2003, la commission des questions juridiques et des droits de l'homme a été saisie d'une proposition de recommandation présentée par M. Bindig et plusieurs de ses collègues[1]demandant que l'on réalise une évaluation précise des implications de l'utilisation des moyens de vidéosurveillance et de leur impact sur le niveau de la criminalité dans les Etats membres.

2. Le 27 avril 2004, la commission des questions juridiques et des droits de l'homme a nommé M[me] Maria Aduarda Azevedo (Portugal, PPE/DC) rapporteuse sur cette question, succédant à M. Ignasi Guardans qui quittait l'Assemblée parlementaire.

3. Le 23 mai 2005, la commission des questions juridiques et des droits de l'homme a nommé M. Yuri Sharandin (Fédération de Russie, GDE) rapporteur sur cette question.

4. La vidéosurveillance désigne les systèmes techniques et électroniques permettant d'assurer la surveillance à distance des biens et des personnes au moyen de caméras vidéo (caméras de télévision en circuit fermé – TVCF). Le développement de cette technologie est venu en réponse au sentiment d'insécurité croissant de l'opinion publique face à la hausse de la criminalité et de la délinquance, et à la demande exprimée auprès des autorités publiques d'un renforcement de la prévention et de la répression des infractions. Le contexte actuel de recrudescence des actes de terrorisme en Europe ne peut qu'alimenter encore l'angoisse sécuritaire de l'opinion publique et n'est pas vraiment de nature à favoriser une inversion de la tendance.

5. La question soulevée ne manquera pas, comme on peut s'y attendre dès lors qu'une innovation technologique touche aux libertés individuelles et à la vie privée, de soulever arguments et commentaires opposés. Il est clair que certains stigmatiseront les risques d'utilisation abusive de cette technologie, au nom du strict respect des droits de l'individu, de sa dignité et de sa vie privée, et fustigeront l'utopie du «tout sécuritaire», quitte à agiter le spectre orwellien du Big Brother. D'autres, au contraire, prôneront la nécessaire limitation de ces droits et libertés individuels au nom de l'intérêt général, de la sécurité publique et de la protection de l'ordre public.

6. Au final, la commission devra répondre à cette question: quelle est l'utilité sociale de la vidéosurveillance? Il s'agit en effet de déterminer si l'usage de cette technologie répond bien aux besoins de nos sociétés et si les législations et réglementations en vigueur garantissent un juste équilibre entre le respect des droits de la personne et des libertés publiques et la limitation de ces mêmes droits, par application du principe de proportionnalité.

7. Le Conseil de l'Europe a été sur cette question particulièrement actif, notamment en adoptant des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance (rapport adopté par le Comité européen de coopération juridique (CDCJ) en mai 2003, reproduit en annexe).

8. Pour élaborer ce rapport, la commission des questions juridiques et des droits de l'homme a organisé le 3 octobre 2006 un échange de vues avec M. Paul Wille, sénateur belge, membre de l'Assemblée. M. Wille a donné des précisions sur le processus législatif relatif à la vidéosurveillance en Belgique où un projet de législation était alors en cours d'examen.

9. A la suite de cet échange de vues, la commission a décidé de demander à la Commission européenne pour la démocratie par le droit (Commission de Venise) de rendre un avis sur la compatibilité de la vidéosurveillance avec les droits de l'homme fondamentaux. La commission s'est notamment intéressée à la question suivante: «A partir de quel moment l'observation normale des gens dans les lieux publics (par des autorités, des institutions ou de simples particuliers) devient-elle un problème juridique et politique du fait que des caméras de surveillance sont utilisées, parfois en réseau?»

10. La Commission de Venise a adopté cet avis lors de sa 70[e] session plénière (16 et 17 mars 2007) sur la base des observations de MM. Pieter Van Dijk, Vojin Dimitrijevic et Giovanni Buttarelli[2].

---

1. Doc. 9869.
2. Avis sur la vidéosurveillance dans les lieux publics par les autorités publiques et la protection des droits de l'homme, premier avis de la Commission de Venise, CDL-AD(2007)014, disponible à l'adresse suivante: http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp.

11. Un avis complémentaire sur la vidéosurveillance dans les sphères publiques et privées par des opérateurs privés et dans la sphère privée par les autorités publiques et la protection des droits de l'homme a été adopté lors de la 71e session plénière de la Commission de Venise (1er et 2 juin 2007)[3].

2. Une technologie banalisée

12. Les premiers systèmes de vidéosurveillance sont apparus à la fin des années 1950 et leur développement a été dopé par l'invention en 1956 de la cassette vidéo. Leur utilisation par des personnes privées s'est généralisée et considérablement banalisée dans les trois décennies suivantes en tant que moyens de surveillance de locaux privés, qu'ils soient accessibles ou non au public, permettant de contrôler la circulation des personnes aux abords, à l'entrée et à l'intérieur des immeubles: commerces de luxe, centres commerciaux, banques, immeubles d'habitation, etc. Ils se sont étendus à la surveillance des lieux de travail et des lieux de loisirs culturels et sportifs. De nos jours, les citoyens sont parfaitement familiarisés avec ces systèmes de surveillance, d'autant mieux acceptés qu'ils répondent à la demande d'un public soucieux de tranquillité et de sécurité.

13. On considère que le Royaume-Uni à lui seul – la patrie d'Orwell paradoxalement – compte 4 millions de caméras de surveillance, soit 10 % des caméras de surveillance dans le monde, ce chiffre ayant quadruplé en trois ans. 85 % des municipalités du Royaume-Uni sont équipées de réseaux de vidéosurveillance. On estime qu'environ 10 millions de vidéocassettes sont enregistrées chaque jour. Un citoyen britannique serait filmé en moyenne plus de 500 fois par semaine, et un Londonien 300 fois par jour!

14. Une étude conduite dans le cadre du projet Urbaneye de la Commission européenne[4]et publiée au printemps 2004 révèle que 90 % des Britanniques interrogés sont favorables à ces dispositifs (contre 48 % des Allemands et 24 % des Autrichiens interrogés). 47 % des Londoniens croient que la vidéosurveillance protège contre la criminalité contre seulement 4 % des Viennois.

15. Ainsi que le montrent les enquêtes ou les sondages d'opinion qui font apparaître des différences de perception selon les pays, la question du degré d'acceptation ou de tolérance de ces systèmes revêt un aspect éminemment culturel. Par ailleurs, il n'est pas certain que la population tolère la vidéosurveillance de la même manière selon qu'elle est utilisée dans un lieu privé ou dans un lieu public.

16. Une enquête conduite en France en 1996 montre que l'acceptabilité sociale varie selon les applications. Seulement 9 % des personnes interrogées considéraient la présence de caméras dans les parkings et les magasins comme une atteinte à la vie privée; en revanche, 51 % estimaient que la diffusion, à leur insu, d'une image prise dans un lieu public constituait une atteinte grave à leur vie privée. A l'inverse, au Royaume-Uni, la majorité de la population accepte de faire davantage de concessions sur ses droits fondamentaux dans un but sécuritaire.

17. A partir des années 1980 et surtout dans les années 1990, la vidéosurveillance a quitté l'espace privé ou semiprivé pour envahir l'espace public. De plus en plus d'organismes publics ont recours à des systèmes de vidéosurveillance pour assurer le contrôle des lieux et bâtiments publics: bâtiments administratifs, installations de défense nationale, prisons, musées, écoles, universités, gares, aéroports, hôpitaux, mais aussi surveillance des frontières.

18. Mais c'est surtout dans le domaine des transports publics et de la régulation de la circulation routière que les moyens de vidéosurveillance ont connu un développement rapide. Le périphérique de Bruxelles est équipé de caméras depuis 1993. Les principaux tunnels des Alpes, d'Espagne et des pays scandinaves sont également équipés. Mais si la vidéosurveillance permet d'assurer la régulation du trafic et la sécurité sur les voies à grande circulation et les carrefours sensibles, elle permet également d'identifier les contrevenants au Code de la route. A Londres, dont l'équipement en caméras a débuté depuis 1974, l'installation, en 2003, du système de péage urbain pour pénétrer dans la ville s'est accompagnée de la mise en place de quelque 700 caméras de contrôle des plaques minéralogiques.

---

3. Avis sur la vidéosurveillance dans les sphères publiques et privées par des opérateurs privés et dans la sphère privée par les autorités publiques et la protection des droits de l'homme, CDL-AD(2007)027, disponible à l'adresse suivante: http://www.venice.coe.int/docs/2007/CDL-AD(2007)027-e.asp. Le rapporteur estime que cela n'entre pas dans le cadre du présent rapport mais que cette question devra être examinée de plus près par l'Assemblée.

4. Cette étude comparative coordonnée par le Zentrum Technik und Gesellschaft (Technische Universität Berlin) sur l'usage de la vidéosurveillance dans les lieux accessibles au public en Europe a été effectuée entre septembre 2001 et février 2004 dans les pays suivants: Autriche, Danemark, Allemagne, Hongrie, Norvège, Espagne et Royaume-Uni, et dans leurs capitales.

19. Plusieurs pays ont également mis en place des systèmes de surveillance dans les moyens de transport public: 5 000 caméras surveillent la totalité des voies, quais et couloirs du métro de Paris. Les réseaux de métros d'Amsterdam, de Stockholm, de Bucarest, de Bruxelles et de Vienne, notamment, sont également équipés en vidéosurveillance. En Suisse, les Chemins de fer fédéraux ont mis en place en 2003 un réseau de vidéosurveillance de leurs installations ferroviaires et des trains. L'aéroport de Francfort est équipé de 2 000 caméras. La vidéosurveillance équipe également plus de 40 gares allemandes.

20. En France, la décision prise en 2003 de mettre en place un système de caméras numériques de surveillance aux points d'entrée et aux abords de quelque 90 collèges de la banlieue parisienne a soulevé un tollé. Pourtant, au Royaume-Uni, plus de 100 écoles sont équipées. C'est également le cas pour les écoles de trois villes du Danemark. Les universités de Cologne, d'Edimbourg, de Dundee, de Cardiff, de Porto et d'Eindhoven, par exemple, possèdent également des équipements de vidéosurveillance.

21. La vidéosurveillance devrait faire également irruption dans les prétoires, le Royaume-Uni envisageant d'installer des caméras dans certaines cours d'appel du pays.

3. Vidéosurveillance et efficacité de la lutte contre la criminalité: une équation contestée

22. L'installation dans les lieux publics de caméras de surveillance est la réponse des autorités publiques au sentiment d'insécurité des citoyens et à leur demande d'une meilleure prévention et d'une plus grande répression de la criminalité. La prolifération de ces systèmes répond à des impératifs sécuritaires: lutter contre la recrudescence des vols, des agressions physiques, du vandalisme, des cambriolages, du trafic de stupéfiants, de la prostitution, etc.

23. Il est clair que l'utilisation de la vidéosurveillance a des applications principalement policières et sert de moyen d'identification visuelle des personnes.

24. La technologie est-elle la clé de la sécurité dans les lieux publics? Les différentes études sur l'impact de la vidéosurveillance sur la délinquance sont en fait pour la plupart contradictoires.

25. Il est vrai que de nombreux exemples démontrent une certaine efficacité de la vidéosurveillance dans la lutte contre la criminalité. Ainsi c'est souvent une caméra de surveillance qui permet l'identification et l'arrestation des criminels et délinquants.

26. L'utilisation de la vidéosurveillance a contribué avec une efficacité impressionnante à l'arrestation des terroristes qui prévoyaient de perpétrer un attentat à la bombe dans le centre de Londres, fin juin 2007. Auparavant, la vidéosurveillance avait révélé son extrême importance lorsqu'il s'était agi d'établir les responsabilités dans les attentats terroristes du métro de Londres, en juillet 2005. En effet, les enregistrements vidéo sur lesquels on voyait les six hommes accusés d'avoir préparé les attentats (qui ont fait 25 morts et 700 blessés) ont été utilisés lors de leur procès. Le 21 juillet 2005, la police a fait savoir que quatre autres terroristes avaient tenté de faire exploser des bombes dans le métro londonien. Ces quatre hommes ont été arrêtés grâce à la diffusion de vidéos sur lesquelles ils apparaissaient.

27. Chacun garde aussi en mémoire le tragique assassinat, dans un grand magasin de Stockholm, en septembre 2003, de la ministre suédoise des Affaires étrangères, Anna Lindh; l'identification et l'arrestation de son meurtrier ont été possibles grâce à la vidéosurveillance. Un fait divers plus récent a eu lieu en avril 2006 avec l'assassinat de Joe Van Holsbeeck à Bruxelles. Ce jeune homme de 17 ans a été poignardé à mort à la gare très fréquentée de Bruxelles-Central. Cette affaire a montré comment la police s'était servie des caméras de vidéosurveillance pour identifier les agresseurs et reconstituer leurs mouvements avant et après le meurtre de Van Holsbeeck.

28. Quelques chiffres tirés d'une enquête française de 1998 vont dans ce sens: dans les agences de banque soumises à la vidéosurveillance, 50 % des voleurs sont identifiés et arrêtés dans les deux ans qui suivent. Dans le métro parisien, 83 % des incidents sont détectés grâce aux caméras de surveillance et le nombre des interpellations a augmenté de 36 %. De même, dans une commune anglaise de 10000 habitants, où six caméras surveillent le centre-ville, le nombre de délits est passé de 137 en 1991 à 37 en 1992. A Monaco, truffée de caméras, le taux de criminalité est trois fois inférieur à celui des Alpes-Maritimes voisines.

29. La Commission de Venise note aussi qu'en raison de l'ampleur des progrès de la technologie, «la vidéosurveillance, à plusieurs égards, est beaucoup plus efficace que l'observation humaine» mais elle conclut toutefois que la vidéosurveillance pourrait être bien plus attentatoire aux droits de l'homme que l'observation humaine[5]. Cela découle notamment de la possibilité de stocker les images et de les transmettre facilement par voie électronique, ce que ne permet pas l'observation humaine.

30. A l'inverse, d'autres études démontrent une inefficacité de la vidéosurveillance en matière de lutte contre la criminalité. Ainsi la vidéosurveillance dans le métro parisien n'a été d'aucun secours dans la lutte contre le terrorisme. La commune de Levallois-Perret est un exemple remarquable d'inefficacité de la vidéosurveillance: ses rues sont parmi les plus surveillées de France et on constate pourtant une augmentation significative de la délinquance.

31. On ne peut donc rien conclure de définitif quant à l'efficacité d'un tel système, et l'un des experts en la matière, le professeur Jason Ditton, directeur du Scottish Centre for Criminology de Glasgow, affirme que rien ne prouve que la vidéosurveillance ait un impact sur le taux de criminalité. Les études conduites dans les années 1990 par le Scottish Centre for Criminology tendent en effet à relativiser l'impact de la vidéosurveillance sur le niveau de la criminalité et le réflexe sécuritaire des citoyens[6].

32. Lors de la 23e Conférence internationale des commissaires à la protection des données et à la vie privée en 2001, a été évoqué le système de reconnaissance automatique faciale associé à un dispositif de vidéosurveillance[7]mis en place à Newham, dans la banlieue de Londres. La ville est équipée depuis 1998 d'un système de vidéosurveillance en circuit fermé couplé à une technologie qui permet d'alerter la police lorsqu'une personne présente dans ses fichiers passe devant une de ces caméras. Lors de l'implantation du dispositif en 1997, 75 % des 250 000 habitants vivaient dans la crainte d'être agressés. Ce taux a été ramené à 67 % en 1998 et a continué à diminuer par la suite. Au début de l'année 1998, un sondage conduit par les autorités locales avait révélé que 67 % des personnes interrogées étaient favorables au système, ce taux ayant même grimpé à 93 % d'opinions favorables à la fin de 1999 (le questionnaire ayant pris soin de demander aux personnes interrogées d'exprimer leur opinion en prenant en considération les conséquences qui pouvaient résulter de la mise en place du dispositif sur les droits de l'homme, les droits civils et la vie privée). Le système de comparaison repose sur les fichiers de la police concernant les personnes condamnées pour crime et impliquées dans de telles affaires au cours des douze dernières semaines. Les fiches des personnes sont examinées par la police au moins toutes les douze semaines. Les visages scannés ne sont pas sauvegardés sauf s'ils correspondent «sans aucun doute» à une personne fichée dans la base de données. Toutes les zones couvertes par le système sont signalées au public. Résultat: une diminution de 34 % de la criminalité depuis 1997.

33. La même technologie associant un système de vidéosurveillance à un dispositif de reconnaissance faciale a également été expérimentée aux Etats-Unis par la ville de Tampa en Floride, en janvier 2001, à l'occasion du Super Bowl (finale du championnat de football américain). Cette expérience a été critiquée par l'ACLU (American Civil Liberties Union) qui, dans une étude[8], concluait que cette technique n'était pas assez fiable pour justifier une mise en application représentant de nombreuses menaces pour la vie privée. Il est vrai que ce système a permis de signaler à plusieurs reprises la présence du terroriste Carlos dans la foule, alors que celui-ci se trouvait en fait à ce moment-là en France où il purgeait une peine de prison. Ce qui pose la question de la fiabilité de ce système de reconnaissance automatique des personnes.

4. Sécurité publique ou contrôle social?

34. Des voix se sont élevées depuis plusieurs années pour dénoncer les dangers de l'instrumentalisation de la sécurité. La vidéosurveillance pose dans des termes renouvelés le problème de la nécessaire conciliation entre l'exercice des libertés individuelles, la liberté d'aller et venir et le droit à la vie privée, et la

---

5. Premier avis de la Commission de Venise, paragraphes 17 et 21. Parmi les exemples cités, la vision de nuit, les possibilités de zoom et de pistage automatique, la reconnaissance vocale et même des dispositifs intelligents de détection de fausses barbes ou de fausses moustaches.

6. Les conclusions de ces études démontrent que, dans l'année qui a suivi l'introduction à Glasgow (570000 habitants), en novembre 1994, de la vidéosurveillance, le taux de criminalité a baissé, mais beaucoup moins que dans d'autres villes non équipées de vidéosurveillance. Ce résultat était davantage imputable à la tendance globale de réduction de la criminalité dans le pays; en données corrigées, la criminalité à Glasgow avait en fait augmenté de 9 %. Des sondages d'opinion ont parallèlement démontré que la vidéosurveillance n'avait eu aucun impact sur le sentiment d'insécurité dans la population. En 1995, les 32 caméras de vidéosurveillance avaient permis 209 arrestations à Glasgow, correspondant à seulement 5 % des crimes commis au centre-ville cette année-là. En revanche, après l'installation en 1992 de 12 caméras à Airdrie (36000 habitants), le taux de criminalité a baissé et le nombre d'identifications a augmenté.

7. Un tel système permet:
   l'identification, par comparaison d'un visage à ceux mémorisés dans une base;
   la vérification, par comparaison des identités déclarées avec les identités associées aux visages mémorisés;
   la supervision, qui permet de suivre l'image d'une personne dans une séquence vidéo;
   la surveillance, qui permet de retrouver, en temps réel, une personne dans une séquence vidéo à partir d'une liste de visages.

8. «Drawing a Blank: The failure of Facial Recognition Technology in Tampa, Florida», janvier 2002.

prévention des atteintes à l'ordre public. L'utilisation banalisée et très répandue de la vidéosurveillance permet de contrôler une population de plus en plus large sans que celle-ci en ait toujours conscience. Dans son principe même, dès lors que l'on oppose sécurité et liberté, la vidéosurveillance présente un risque d'ingérence dans la vie quotidienne des citoyens et d'atteinte au droit au respect de leur vie privée. En second lieu se pose le problème des conditions de collecte, d'utilisation et de diffusion des informations et données collectées sur les individus (sous la forme d'images et de sons) par la vidéosurveillance. La vidéosurveillance permet d'identifier, directement (reconnaissance du visage) ou indirectement (par son véhicule, son habillement, etc.), les personnes. Elle permet de multiplier les informations sur leur comportement, leurs déplacements et leurs activités. La collecte de telles données permet un véritable traçage des personnes.

35. Selon deux avocats belges, auteurs d'un rapport sur la vidéosurveillance en Belgique, la vidéosurveillance menace la vie privée de deux façons: lorsqu'elle s'opère de manière secrète, elle conduit à soustraire des informations, consistant en certains comportements ou attitudes, que l'intéressé aurait pu ne pas souhaiter divulguer; lorsqu'elle est connue des personnes concernées, la vidéosurveillance les incite à adopter certains comportements ou attitudes, plus ou moins éloignés des comportements qui seraient véritablement les leurs en l'absence de la surveillance. Ce dernier constat est à relier avec le phénomène de déplacement de la criminalité, depuis les rues et quartiers équipés de caméras vers ceux qui en sont dépourvus. Cela remet dans une certaine mesure en cause l'efficacité de la vidéosurveillance dans la lutte contre la délinquance.

36. La Commission de Venise est parvenue à cette même conclusion: «En principe, avant de pénétrer dans un lieu public, une personne modifiera son apparence et sa conduite étant donné qu'elle pourra y être observée par autrui.» Elle rappelle cependant que, même si le degré d'intimité est nécessairement moindre dans les lieux publics, la personne n'y est pas pour autant «privée de ses droits et libertés, y compris ceux se rapportant à sa sphère privée et à son image»[9].

37. Les caméras sont de plus en plus performantes: elles peuvent surveiller un champ de vision sur 360 degrés; munies de zooms, elles sont capables par exemple de lire un journal à plus de 100 mètres de distance ou une plaque minéralogique à 300 mètres. Certaines comportent des détecteurs qui donnent l'alerte en cas d'incident ou de signes d'anormalité dans leur champ de vision: fumée suspecte, mouvement brusque… On a pu dire que dans Oxford Street à Londres, les caméras étaient capables d'identifier la pointure des chaussures des passants.

38. Les techniques des systèmes de vidéosurveillance se rapprochent de plus en plus d'autres technologies qui font naître de nouvelles préoccupations relatives à la protection de la vie privée et des données. Elles comprennent, entre autres, les enregistrements sonores, les réseaux informatiques sans fils et à haut débit utilisés pour le transfert des images, les systèmes de reconnaissance automatique du visage intégrés à des bases de données informatisées qui peuvent identifier les personnes ou suivre leur trace, et les appareils qui permettent de «voir» derrière les vêtements et les murs, par exemple les dispositifs de reconnaissance thermique ou infrarouge. La transmission des images par les réseaux téléphoniques grand public peut permettre de voir et d'écouter par-delà les frontières, à l'échelle de la planète.

39. Les informations enregistrées peuvent être analysées de manière précise. Il est possible de mettre en place des systèmes d'identification entièrement automatiques, reposant sur les technologies de zoom et d'imagerie numérique, et reliés à d'autres bases de données numériques. C'est ainsi, par exemple, qu'à Bradford, au Royaume-Uni, la vidéosurveillance est reliée à un système de reconnaissance automatique des plaques numérologiques (ANPR – *automatic number plate recognition*) qui permet d'alimenter automatiquement les fichiers de police à raison de 3 000 numéros d'immatriculation relevés par heure et par caméra. Le ministère de l'Intérieur britannique envisage de développer l'usage de cette technologie et d'en équiper les voitures de police.

40. L'évolution technologique dans le domaine de la vidéosurveillance – ANPR, reconnaissance faciale automatique, etc. – renvoie à d'autres interrogations encore. De quelle manière et par quelle procédure est alimentée la base de suspects? Qu'est-ce qu'un suspect? Quand un suspect quitte-t-il la base de données? Comme le souligne à juste titre la Commission de Venise, «en général, ce n'est pas la surveillance en tant que telle qui pose le plus de problèmes, mais l'enregistrement des données et leur traitement (…)»[10]. La

---

9. Premier avis de la Commission de Venise, paragraphe 25. A cet égard, la Commission de Venise souligne à juste titre que la Cour européenne des Droits de l'Homme a considéré, au paragraphe 56 de l'arrêt qu'elle a rendu le 25 septembre 2001 dans l'affaire *P.G. et J.H. c. Royaume-Uni*, qu'il «existe [donc] une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la "vie privée"».
10. Voir le premier avis de la Commission de Venise, paragraphe 29.

protection des données à caractère personnel est en cause et la Commission de Venise rappelle que cette question relève de la protection de la vie privée au sens de l'article 8 de la Convention européenne des Droits de l'Homme[11].

41. L'usage des caméras de vidéosurveillance présente également un risque de discrimination. Les études ont démontré que les agents chargés de visionner les écrans de surveillance tendent à se focaliser plus facilement sur certaines catégories de population. Le processus de reconnaissance faciale automatique, basé sur l'image du visage, renforce davantage la crainte de dérives graves liées au délit de faciès ou encore au délit de pauvreté ou au délit de comportement déviant.

42. La vidéosurveillance peut donner lieu à de nombreux abus qu'il est toujours difficile de prévenir. La finalité du système de surveillance peut facilement être détournée par l'instauration d'un contrôle social: les caméras installées dans un commerce pour prévenir les vols sont souvent utilisées pour surveiller le personnel; les grands magasins s'en servent pour faire des études comportementales sur les consommateurs. Dans un registre plus grave, la vidéosurveillance peut permettre d'assurer un contrôle politique: les caméras installées à Pékin, place Tian'anmen, ont servi à identifier et à arrêter des opposants au régime en juin 1989.

Un cas particulier: les webcams

43. Enfin, il faut également s'intéresser à l'usage qui est fait de la vidéosurveillance dans les lieux publics non pas par des organismes publics mais par des personnes privées pour observer des lieux publics. La prolifération des images prises en direct par des caméras vidéo (webcam) accessibles sur internet pose des problèmes similaires de respect de la vie privée et de conformité avec les règles de la protection des données. Toutefois, le problème se pose non seulement par rapport au traitement des données mais surtout au regard de la diffusion des données et du droit à la personnalité et à l'image.

44. Les webcams sont installées en général dans des lieux publics, souvent sur des sites touristiques. Elles peuvent donner une image fixe ou au contraire changer d'angle de vue, et être munies d'un zoom. Leurs images sont accessibles dans le monde entier; elles sont donc traitées, enregistrées, imprimées et transmises sans aucun contrôle. Pour que ces caméras soient utilisées de manière légale, il faudrait qu'elles soient installées et configurées de manière à ce qu'aucune personne ne soit identifiable, ou que les personnes concernées donnent leur consentement à être filmées. Mais est-ce bien toujours le cas? Selon la position et la qualité technique de la caméra, il est possible de reconnaître une personne filmée; cette personne n'a pas conscience, ni connaissance du fait qu'elle est filmée et que son image sera captée dans le monde entier par le biais d'internet.

45. Il n'est donc pas certain que les législations existantes sur la protection des données et le respect de la vie privée soient, dans ce cas précis, suffisantes à garantir les droits de la personne.

5. Prévenir les dérives en définissant un cadre juridique efficace basé sur le respect d'un certain nombre de principes

46. Face aux dérives potentielles ou aux abus réels, le citoyen européen n'est pas totalement démuni. Des instruments juridiques existent. Au niveau national d'abord, rares sont les Etats qui ont opté pour une législation spécifique concernant la surveillance des lieux privés ou lieux publics par les moyens électroniques. En revanche, nombre d'Etats membres ont des dispositions législatives et constitutionnelles qui trouvent à s'appliquer dans ce domaine, en particulier celles qui garantissent le respect de la vie privée, de la dignité humaine, ou celles qui concernent la protection des données à caractère personnel. Au niveau supranational, plusieurs instruments internationaux couvrent les mêmes domaines, en particulier ceux du Conseil de l'Europe. On peut cependant se demander si ces instruments sont suffisants pour assurer une protection adéquate des citoyens «surveillés».

5.1. Les instruments du droit européen

47. Les activités de vidéosurveillance impliquant le traitement de données à caractère personnel entrent dans le champ d'application de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981 du Conseil de l'Europe (STE n° 108)[12].

11. *Ibid.*, paragraphe 41.

48. La convention est le premier instrument international contraignant qui a pour objet de renforcer la protection juridique des personnes contre l'usage abusif du traitement automatisé des 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. Ces principes portent notamment sur le caractère licite et loyal de la collecte et du traitement automatisé des données, enregistrées pour des finalités déterminées et légitimes et non utilisées à des fins incompatibles avec ces finalités, ni conservées au-delà de ce qui est nécessaire. 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, aux condamnations pénales, etc., en l'absence de garanties offertes par le droit interne. La convention garantit également le droit des personnes concernées de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications.

49. Cette convention a été complétée par un protocole additionnel (STE n° 181) concernant les autorités de contrôle et les flux transfrontières de données, qui est entré en vigueur le 1er juillet 2004.

50. Afin d'adapter les principes généraux énoncés dans la convention aux exigences spécifiques des différents secteurs d'activité de la société, plusieurs recommandations complémentaires ont été adoptées par le Comité des Ministres du Conseil de l'Europe. On mentionnera la Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, la Recommandation n° R (91) 10 sur la communication à des tierces personnes de données détenues par des organismes publics, et la Recommandation n° R (99) 5 sur la protection de la vie privée sur internet.

51. Il n'existe pas d'instrument juridique de l'Union européenne sur la vidéosurveillance proprement dite. La vidéosurveillance des lieux publics ne relève que partiellement de la Directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données, dans la mesure où elle exclut elle-même explicitement de son champ d'application certaines activités de vidéosurveillance, précisément celles qui nous intéressent ici[13].

52. Sous cette réserve, les citoyens communautaires bénéficient tout de même des garanties prévues par cette directive. Tous les pays de l'Union ont transposé cette Directive 95/46/CE, sauf la France. Elle a été complétée par les Directives 97/66/CE et 2002/58/CE sur la vie privée et les communications électroniques. Il n'y a encore pas eu de jurisprudence de la Cour de justice des Communautés européennes (CJCE) concernant la vidéosurveillance. Toutefois, la CJCE reconnaît l'application d'un principe de proportionnalité et la nécessité d'un intérêt public pour opérer une restriction à un droit fondamental.

5.2. Législations des Etats membres

53. Peu de pays comptent dans leur droit des législations réglementant spécifiquement l'emploi de la vidéosurveillance, encore moins de la vidéosurveillance dans les lieux publics. Toutefois, les systèmes juridiques des Etats membres ne sont pas entièrement dépourvus de règles dans ce domaine, puisque les législations sur la protection de la vie privée, sur l'enregistrement et l'utilisation d'informations et de données à caractère personnel, sur le secret ou la confidentialité d'informations sensibles, etc., peuvent s'appliquer aux activités de vidéosurveillance et offrir une base de garanties aux citoyens.

54. L'Espagne est un des rares pays à avoir adopté une législation sur la vidéosurveillance des lieux publics. Cette loi prévoit notamment un mécanisme d'autorisation d'implantation par les entités publiques. Ce pays est parvenu à un niveau élevé d'intégration des systèmes de vidéosurveillance (TVCF) avec les services d'urgence et de sécurité nationaux.

55. En 2006 a été créé à Madrid un centre (Centro Integrado de Seguridad y Emergencias) au sein duquel opèrent en bonne intelligence les différents services de sécurité et d'urgence (police, secours, pompiers, etc.). En cas d'urgence, il est possible d'y déployer une cellule de crise en quelques minutes.

56. L'expérience espagnole a montré la grande efficacité des centres de ce type. Le système municipal intégré de sécurité de Madrid est reconnu comme le meilleur d'Europe.

---

12. Voir l'état des signatures et ratifications: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=11/19/2007&CL=FRE; (le 19 novembre 2007, 38 Etats membres ont ratifié la convention et 5 l'ont signée).

13. Paragraphe 16: «considérant que les traitements des données constituées par des sons et des images, tels que ceux de vidéosurveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en œuvre à des fins de sécurité publique, de défense, de sûreté de l'Etat ou pour l'exercice des activités de l'Etat relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire;».

57. En Espagne, les images des systèmes de vidéosurveillance sont diffusées sur des écrans visibles par tous dans le métro ou les gares par exemple. Cela permet d'associer les citoyens au processus d'observation vidéo et leur rappelle que ces lieux sont sous surveillance. Selon les psychologues, cette transparence, alliée à la signalisation (au moyen de pictogrammes définis par la loi), permet de détendre l'atmosphère et d'établir des conditions favorables à la prévention de la criminalité dans les lieux publics placés sous vidéosurveillance.

58. En Belgique, le sénateur Stefaan Norielde a présenté en avril 2006 une proposition de loi visant à réglementer l'installation et l'usage de caméras de vidéosurveillance.

59. En Grande-Bretagne, environ 5 millions de caméras de TVCF seront en fonction prochainement. Chacun sait que le citoyen ordinaire de la ville de Londres est soumis à une vidéosurveillance 300 fois par jour. Mille soixante caméras de vidéosurveillance fonctionnent dans le seul quartier de Westminster.

60. Afin de maximiser le potentiel du réseau national de vidéosurveillance, un projet de stratégie nationale concernant les systèmes de télévision en circuit fermé est en cours d'élaboration. Les experts britanniques sont parvenus à la conclusion qu'en l'absence d'une telle stratégie, il est probable que les systèmes installés dans les lieux publics du Royaume-Uni resteraient non coordonnés, disparates, de qualité douteuse, moins efficaces et mal ciblés. De plus, faute d'une telle stratégie, il serait peu probable que le Trésor accepte de continuer à financer de tels équipements sur les fonds publics. Il existe donc un danger de voir l'infrastructure actuelle se détériorer et la société perdre la possibilité de maximiser l'efficacité de systèmes de vidéosurveillance, ainsi que d'intégrer des technologies futures pouvant apporter une aide considérable à la police.

61. En France, la vidéosurveillance est réglementée spécifiquement. L'installation, sur la voie publique et dans les lieux ou établissements ouverts au public, de systèmes de vidéosurveillance est réglementée par les dispositions de la loi du 21 janvier 1995 et du décret du 17 janvier 1996. La loi prévoit que les dispositifs ne peuvent être mis en place dans les lieux publics que pour des finalités précises (protection des bâtiments et installations publics, régulation du trafic routier, constatation des infractions aux règles de la circulation et prévention des atteintes à la sécurité des personnes et des biens). L'installation de tels dispositifs est subordonnée à une autorisation préalable. Les dispositifs de vidéosurveillance ne doivent pas permettre de visualiser les images de l'intérieur des immeubles d'habitation ni celles de leurs entrées. La loi prévoit également un droit d'information du public, un droit d'accès des personnes aux enregistrements les concernant, et la destruction des enregistrements dans un délai maximal d'un mois (sauf enquête de flagrant délit ou information judiciaire).

62. Des lois générales sur la protection des données sont envigueur dans plusieurs Etats membres, soit à la suite de la ratification de la convention européenne (STE n^{o} 108), soit pour transposer la Directive 95/46/CE. C'est le cas dans les pays suivants: l'Albanie, l'Autriche, la Belgique, la Bulgarie, Chypre, la République tchèque, le Danemark, l'Estonie, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Islande, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, les Pays-Bas, la Norvège, la Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, l'Espagne, la Suède, la Suisse et le Royaume-Uni, mais aussi l'Azerbaïdjan, la Bosnie-Herzégovine, Malte, Monaco, Saint-Marin, la Serbie-Monténégro et «l'ex-République yougoslave de Macédoine», bien que ces derniers Etats ne soient pas parties à la convention STE n^{o} 108.

Dans 33 Etats membres, c'est la Constitution qui pose le principe fondamental du droit à la vie privée ou à la protection des données. La protection des données figure en tant que droit fondamental dans la Constitution portugaise de 1976, et son article 35 accorde des garanties très complètes au citoyen (droit d'accès aux informations nominatives et droit d'information et de rectification, etc.).

63. Par ailleurs, une majorité d'Etats membres a établi une autorité indépendante de régulation et de contrôle, afin de veiller au respect des principes qui figurent dans leur législation[14].

---

14. Büro der Datenschutzkommission und des Datenschutzrates en Autriche, Commission de la protection de la vie privée en Belgique, Personal Data Protection Commission en Bulgarie, Bureau pour la protection des données à caractère personnel en République tchèque, Office of the Personal Data Protection Commissioner à Chypre, Datatilsynet au Danemark, Data Protection Inspectorate en Estonie, Office of the Data Protection Ombudsman en Finlande, Commission nationale de l'informatique et des libertés en France, Bundesbeauftragte für den Datenschutz en Allemagne, Data Protection Commission en Grèce, Hungarian Data Protection Commissioner en Hongrie, Persónuvernd en Islande, Data Protection Commissioner en Irlande, Garante per la protezione dei dati personali en Italie, State Date Inspection en Lettonie, State Data Protection Inspectorate en Lituanie, Liechstensteinische Landesverwaltung Stabstelle für Datenschutz au Liechtenstein, Commission nationale de la protection des données au Luxembourg, Office of the Commissioner for Data Protection à Malte, College Bescherming Persoonsgegevens aux Pays-Bas, Datatylsinet en Norvège, Office of the

5.3. Jurisprudence de la Cour européenne des Droits de l'Homme[15]

64. La vidéosurveillance relève du champ d'application de l'article 8 de la Convention européenne des Droits de l'Homme (droit au respect de la vie privée – «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance»). La Cour a défini dans sa jurisprudence les limites de l'exercice de ce droit, et, plus particulièrement, dans quelle mesure les autorités publiques étaient en droit d'interférer. Il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice du droit à la vie privée que pour autant que cette ingérence est prévue par la loi et constitue une mesure qui, dans une société démocratique, est nécessaire à la défense d'un certain nombre de buts légitimes. Dans un arrêt (*M.S. c. Suède* du 27 août 1997), la Cour «rappelle que la protection des données à caractère personnel (...) revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention».

65. Dans l'arrêt *Peck c. Royaume-Uni* du 28 janvier 2003, la Cour s'est trouvée saisie pour la première fois du problème de l'atteinte à la vie privée par la vidéosurveillance. En l'espèce, le requérant avait été filmé par une caméra de télésurveillance communale alors qu'il tentait de se suicider, ce qui a conduit à l'intervention de la police. Les images ont été utilisées par la mairie pour une diffusion dans la presse et sur une chaîne de télévision nationale, pour la promotion de la prévention de la criminalité, sans masquer l'identité du requérant. La Cour a jugé que la divulgation de séquences filmées par une caméra de surveillance portait atteinte au droit du requérant à la vie privée, sans raisons pertinentes ou suffisantes pouvant la justifier. La Cour a conclu à la violation de l'article 8 de la CEDH.

66. Pour la Cour, «la surveillance des faits et gestes d'un individu dans des lieux publics par le biais de matériel photographique/visuel sans enregistrement des données visuelles ne constitue pas en soi une ingérence dans la vie privée de l'individu concerné». Cependant la vidéosurveillance doit respecter les critères de légalité, de légitimité et de proportionnalité exprimés dans l'article 8, paragraphe 2, de la Convention. La Cour estime que

> *«la scène a été vue dans une mesure excédant largement ce qu'un passant aurait pu voir ou ce qui aurait pu être observé à des fins de sécurité, et au-delà de ce que l'intéressé aurait pu prévoir alors qu'il marchait à Brentwood, le 20 août 1995». En conséquence, la Cour conclut qu'il y a bien eu atteinte grave à la vie privée du requérant, relevant que «la divulgation des images saisies n'a pas été assortie de garde-fous suffisants pour empêcher une divulgation incompatible avec les garanties relatives au respect de la vie privée du requérant qui découlent de l'article 8».*

67. Signalons qu'il ne s'agit pas de la seule affaire de vidéosurveillance concernant le Royaume-Uni. Dans l'affaire *Martin c. Royaume-Uni* (n° 63608/00), la requérante, Janette Martin, résidant à Nottingham, se plaignait au regard des articles 8 (droit au respect de la vie familiale) et 14 (interdiction de la discrimination) de la Convention de la décision du conseil municipal de sa ville de placer son domicile sous vidéosurveillance, à son insu, à la suite de plaintes de ses voisins concernant son comportement et celui de ses enfants. L'affaire s'est conclue par un règlement amiable.

5.4. Promouvoir dans le droit national des Etats membres des garanties suffisantes

68. Face au développement croissant des technologies de vidéosurveillance, il serait souhaitable de promouvoir une harmonisation des législations des Etats membres dans ce domaine. Il est nécessaire que le droit des Etats membres s'inspire clairement des principes et garanties qui découlent des instruments du Conseil de l'Europe, notamment en ce qui concerne le droit à la vie privée et la protection des données.

69. Le Comité européen de coopération juridique (CDCJ) du Conseil de l'Europe a adopté, en mai 2003, un rapport contenant des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance (voir l'annexe). Il est important que l'Assemblée parlementaire appelle formellement les Etats membres du Conseil de l'Europe à faire application de ces principes et à veiller à ce qu'ils soient respectés de manière aussi systématique que possible.

General Inspector of Data Protection en Pologne, Commissão Nacional de Protecção de Dados au Portugal, Commissioner for Personal Data Protection en Slovaquie, Agencia de Protección de Datos en Espagne, Datainspektionen en Suède, Préposé fédéral à la protection des données en Suisse, Information Commissioner au Royaume-Uni, etc.

15. Pour plus d'informations, le rapporteur attire l'attention du lecteur sur les paragraphes 26 à 33 et 49 à 67 du premier avis de la Commission de Venise

70. Les législations nationales devraient reconnaître les garanties minimales suivantes:

– le principe de la légalité ou licéité: la vidéosurveillance ne peut être effectuée que si elle est autorisée par la loi, justifiée par un intérêt public ou privé prépondérant et bénéficie du consentement des personnes concernées;

– le principe de la proportionnalité: la vidéosurveillance doit être un moyen adéquat et nécessaire à la réalisation de l'objectif poursuivi, à savoir la sécurité, notamment la protection contre les atteintes aux biens et/ou aux personnes. Elle ne peut être retenue que si d'autres mesures moins attentatoires à la vie privée s'avèrent insuffisantes ou impraticables. L'installation d'une caméra doit être effectuée de façon à ce que n'entrent dans son champ que les images strictement nécessaires à la surveillance envisagée;

– le principe de la finalité ou de la légitimité: les données ne peuvent être utilisées que dans le cadre de la protection contre les atteintes aux biens et aux personnes. Elles ne peuvent donner lieu à d'autres utilisations (notamment commerciales). La communication de données personnelles enregistrées par une caméra est interdite sauf dans les cas prévus ou autorisés par la loi;

– le principe de la publicité ou de l'information: l'existence d'un système de vidéosurveillance doit être portée à la connaissance du public; le responsable du système de vidéosurveillance doit informer les personnes entrant dans le champ des caméras de surveillance de l'utilisation d'un tel système par le biais d'un avis lisible;

– le principe du contrôle: les personnes directement concernées par les informations collectées ainsi que les autorités publiques de régulation doivent être en mesure de s'assurer que les droits des personnes sont respectés par les utilisateurs;

– le principe du droit d'accès aux données des personnes concernées: les personnes concernées doivent avoir connaissance de la teneur de l'information qu'un fichier contient éventuellement sur son compte;

– le principe du droit de rectification d'une information erronée ou inappropriée par les personnes concernées;

– un droit de recours si l'un des éléments précédents n'est pas respecté: toute personne concernée doit pouvoir défendre ses droits afin de lui permettre d'exercer un contrôle sur les informations la concernant, lorsqu'elles sont recueillies, traitées et diffusées le cas échéant;

– la garantie de la sécurité des données: le responsable du système de vidéosurveillance doit prendre les mesures appropriées d'accès et de conservation afin de protéger les données personnelles contre tout traitement non autorisé. La durée de conservation des données et des enregistrements doit être limitée.

6. Conclusions

71. Plusieurs instruments juridiques, au niveau national comme au niveau européen, offrent des garanties minimales concernant la protection des droits des citoyens au regard de la vidéosurveillance. En l'état actuel de la réflexion, une convention européenne ou une recommandation du Comité des Ministres du Conseil de l'Europe sur la vidéosurveillance n'aurait guère de valeur ajoutée par rapport aux instruments existants. Toutefois, les législations nationales n'étant pas homogènes dans ce domaine, il est important que l'Assemblée parlementaire appelle formellement les Etats membres du Conseil de l'Europe à appliquer les principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance figurant dans le rapport du CDCJ de 2003, et à veiller à ce que ces principes soient respectés de manière aussi systématique que possible.

72. Il faudrait adopter dans tous les Etats membres un signe uniformisé (pictogramme) indiquant les lieux placés sous vidéosurveillance.

73. Le signe (pictogramme) devrait être accompagné d'un texte uniformisé rappelant la législation.

74. Les équipements informatiques et de vidéosurveillance existants permettent l'utilisation de zooms très puissants (facteur de grossissement jusqu'à 30x-50x) et d'une très haute résolution d'image. Les Etats membres du Conseil de l'Europe devraient adopter une législation limitant l'installation de ces équipements en fonction de la spécificité des lieux concernés.

75. Les équipements informatiques et de vidéosurveillance existants permettent de soustraire automatiquement à l'observation vidéo des «zones privées» (les fenêtres d'appartements, par exemple). Cette pratique permet non seulement de protéger la vie privée en général mais aussi de préserver les employés de centres de vidéosurveillance de la vision de scènes qui ne relèvent pas de leur compétence. Dans les pays membres du Conseil de l'Europe, il conviendrait de définir légalement ces «zones privées» et de faire en sorte que, grâce à l'utilisation de logiciels adaptés, elles échappent à la vidéosurveillance.

76. Actuellement, les images des caméras de vidéosurveillance sont stockées au format numérique et il est possible de les protéger par chiffrement, ce qui empêche, le cas échéant, la consultation des informations stockées par des tiers, les accès non autorisés et d'éventuelles modifications. Le chiffrement est nécessaire pour que la validité des informations soit reconnue dans le cadre des enquêtes criminelles. Dans les Etats membres du Conseil de l'Europe, la pratique du chiffrement des données vidéo devrait être imposé par la loi.

77. Toute personne vivant dans un espace sous vidéosurveillance a le droit de se savoir surveillée. Les pays membres du Conseil de l'Europe devraient donc inscrire ce droit dans leur législation.

78. La coopération entre les organismes gouvernementaux et les structures non gouvernementales est indispensable dans le domaine de la vidéosurveillance.

79. Pour mettre à jour et compléter les informations dans ce domaine, il serait souhaitable que le Conseil de l'Europe organise une conférence à laquelle pourraient être invités différents experts:

– des spécialistes de la vidéosurveillance issus du secteur public et du secteur privé;

– des représentants de centres de recherche universitaire ou d'organes de suivi ayant mené récemment des études sur des sujets tels que les répercussions de la vidéosurveillance sur le taux de criminalité ou les aspects relatifs à la vie privée;

– des représentants des comités d'experts compétents du Conseil de l'Europe (CDCJ, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – T-PD);

– des représentants d'autorités nationales de réglementation ou d'observation de la protection des données ou de la vie privée;

– des représentants de la société civile (d'associations comme Privacy International, par exemple).

Annexe – Rapport contenant des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance (2003), adopté par le Comité européen de coopération juridique (CDCJ), lors de sa 78e réunion (20-23 mai 2003)[16]

Commission chargée du rapport: commission des questions juridiques et des droits de l'homme.

Renvoi en commission: Doc. 9869 et Renvoi no 2864 du 8 septembre 2003.

Projet de résolution et projet de recommandation adoptés à l'unanimité par la commission le 13 décembre 2007.

Membres de la commission: M. Dick Marty (Président), M. Erik **Jurgens**, M. György **Frunda**, Mme Herta DäublerGmelin (Vice-Présidents), M. Miguel Arias, Mme Aneliya **Atanasova**, M. Abdülkadir **Ateş**, M. Jaume Bartumeu Cassany, Mme Meritxell Batet, Mme Marie-Louise **Bemelmans-Videc**, Mme Anna **Benaki**, M. Luc **Van den Brande**, M. Erol Aslan Cebeci, Mme Pia Christmas-Møller, Mme Ingrīda **Circene**, Mme Alma Čolo, M. Joe Costello (remplaçant: M. Terry **Leyden**), Mme Lydie **Err**, M. Valeriy **Fedorov**, M. Aniello Formisano, M. Jean-Charles Gardetto, M. József Gedei, M. Valery Grebennikov, Mme Carina Hägg, M. Holger **Haibach**, Mme Gultakin Hajiyeva, Mme Karin Hakl, M. Andres **Herkel**, M. Serhiy **Holovaty**, M. Michel Hunault (remplaçant: M. Michel **Dreyfus-Schmidt**), M. Rafael Huseynov, Mme Fatme Ilyaz, M. Kastriot Islami, M. Željko Ivanji, Mme Kateřina Jacques, M. Karol Karski, M. Hans Kaufmann, M. András Kelemen, Mme Kateřina Konečná, M. Nikolay Kovalev (remplaçant: M. Yuri **Sharandin**), M. Eduard Kukan, Mme Darja Lavtižar-Bebler, M. Andrzej Lepper, Mme Sabine **Leutheusser-Schnarrenberger**, M. Humfrey **Malins**, M. Andrija Mandić, M. Pietro Marcenaro (remplaçant: M. Andrea **Manzella**), M. Alberto Martins (remplaçant: M. Ricard **Rodrigues**), M. Andrew **McIntosh**, M. Murat Mercan, Mme Ilinka Mitreva, M. Philippe **Monfils**, M. João Bosco Mota Amaral, M. Philippe **Nachbar**, Mme Nino Nakashidzé, M. Fritz Neugebauer, M. Tomislav Nikolić, M. Anastassios Papaligouras, M. Ángel Pérez Martínez, M. Claudio Podeschi, M. Ivan Popescu, Mme Maria Postoico, Mme Marietta **de Pourbaix-Lundin**, M. Christos **Pourgourides**, M. John **Prescott**, M. Jeffrey Pullicino Orlando, M. Valeriy Pysarenko, Mme Marie-Line **Reynaud**, M. François Rochebloine (remplaçant: M. Germinal **Peiro**), M. Francesco Saverio Romano, M. Paul Rowen (remplaçant: M. Christopher **Chope**), M. Armen Rustamyan (remplaçant: M. Raffi **Hovannisian**), M. Kimmo **Sasi**, M. Ellert Schram, M. Christoph Strässer, M. Mihai Tudose, M. Vasile Ioan Dănuţ **Ungureanu**, M. Øyvind **Vaksdal**, M. Egidijus Vareikis, Mme Renate Wohlwend, M. Marco Zacchera, M. Krzysztof **Zaremba**, M. Vladimir Zhirinovsky, M. Miomir Žužul.

N.B. Les noms des membres présents à la réunion sont indiqués en gras.

Voir 9e séance, 25 janvier 2008 (adoption des projets de résolution et de recommandation); et Résolution 1604 et Recommandation 1830.

16. Ce document est disponible sur le site internet du Conseil de l'Europe à l'adresse suivante: www.coe.int.