Strasbourg, le 23 mars 2007 **CDL-AD(2007)014**

Étude No. 404 / 2006 Or. angl.

COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT

(COMMISSION DE VENISE)

AVIS

SUR LA VIDÉOSURVEILLANCE DANS LES LIEUX PUBLICS PAR LES AUTORITÉS PUBLIQUES ET LA PROTECTION DES DROITS DE L'HOMME

adopté par la Commission de Venise
lors de sa 70e session plénière
(Venise, 16-17 mars 2007)

sur la base des observations de

M. Pieter van DIJK (Membre, Pays-Bas)
M. Vojin DIMITRIJEVIC (Membre, Serbie)
M. Giovanni BUTTARELLI (Expert, Italie)

TABLE DES MATIÈRES

I. *Introduction*

1. Par lettre datée du 10 octobre 2006, le Président de la Commission des affaires juridiques et des droits de l'Homme de l'Assemblée parlementaire, M. Dick Marty, a sollicité l'avis de la Commission de Venise sur la question de savoir « dans quelle mesure la vidéosurveillance est compatible avec les droits fondamentaux ». La Commission des affaires juridiques a notamment soulevé la question suivante : « à partir de quel moment l'observation normale des gens dans les lieux publics (par des autorités, des institutions ou de simples particuliers) devient un problème juridique et politique du fait que des caméras de surveillance sont utilisées, parfois en réseau ? »

2. MM. Pieter van Dijk (CDL(2007)010) et Vojin Dimitrijevic (CDL(2007)011) ont été nommés rapporteurs. En outre, pour bien cerner les questions se rapportant à la protection des données à caractère personnel dans le cadre de la vidéosurveillance, les observations d'un expert ont été sollicitées. C'est ainsi que M. Giovanni Buttarelli (CDL(2007)012), Secrétaire général de l'Autorité italienne de contrôle de la protection des données, a été prié de contribuer à la présente étude.

3. Cette étude, établie sur la base de leurs observations, a été adoptée par la Commission de Venise lors de sa 70e session plénière (Venise, 16-17 mars 2007).

1. Champ de l'étude

4. La présente étude porte sur l'observation des personnes dans les lieux publics par les autorités publiques au moyen d'outils de vidéosurveillance, quel qu'en soit le type, qu'ils soient connectés ou non à un réseau, et que les données rassemblées soient enregistrées ou non. Cette étude examine les pratiques les plus courantes au regard des règles et normes européennes en matière de droits de l'homme.

5. Compte tenu du bref délai qui lui était imparti, la Commission de Venise ne pouvait que tirer des conclusions préliminaires, qui en aucun cas ne doivent être considérées comme complètes ou définitives. La Commission entend pousser plus avant sa réflexion afin d'établir des lignes directrices permettant de mettre en balance les intérêts publics concernés par rapport aux libertés et droits fondamentaux de chacun dans une société démocratique. À cet égard, les questions de la vidéosurveillance opérée par des agents privés et de la vidéosurveillance des lieux privés par les autorités publiques méritent elles aussi d'être étudiées. Toutefois, les points de droit que ces questions soulèvent ne sont pas les mêmes et seront examinés dans un avis ultérieur de la Commission de Venise.

6. Afin de délimiter le champ de l'étude, il y a lieu de définir les termes et notions qui y sont visés.

2. Autorités publiques

7. La présente étude examine les questions de droit que soulèvent les systèmes de vidéosurveillance utilisés par les autorités publiques dans le cadre de l'exécution par l'État de son obligation d'assurer la sécurité, de maintenir l'ordre public et de protéger les droits et libertés de tous. Cette étude vise donc les autorités nationales ou locales lorsqu'elles exercent leurs activités de prévention et de protection, ou celles se rapportant à la répression des infractions pénales. Aussi cette étude ne concerne-t-elle pas les opérations de vidéosurveillance menées par les autorités publiques aux fins de la défense nationale, ni les systèmes de vidéosurveillance mis en place par les personnes physiques ou les personnes

morales de droit privé telles que les banques, les casinos ou les établissements commerciaux ou semi-publics.

3. Lieux publics

8. Un lieu public est un endroit auquel quiconque, en principe, peut accéder librement, sans distinction, à tout moment et en toutes circonstances. Les lieux publics sont ouverts au public. En principe, ils peuvent être utilisés par tous à tout moment et librement. Les lieux publics sont régis par les autorités publiques, dont les pouvoirs en matière d'intervention et d'application de la loi y sont plus étendus que dans les lieux privés.

9. Parmi les exemples de lieux publics pris en compte dans la présente étude, il y a les parcs publics, les rues piétonnes des centres-villes, les parcs de stationnement extérieurs, les rues des quartiers résidentiels, ou des secteurs tels que les stades de sport et les stations de métro. Certains lieux publics tels que les universités, les discothèques ou les cafés, qui peuvent être considérés comme des lieux semi-publics, sont eux aussi pris en compte.

4. Sphère privée

10. La sphère privée, au sens concret, est un domaine dont l'accès peut être restreint par la loi et par les personnes qu'elle protège. La sphère privée, en principe, n'est pas librement ouverte au public et n'est pas accessible à tous, à tout moment, en toutes circonstances ni sans distinction. Les règles régissant la sphère privée relèvent principalement du droit privé. Les pouvoirs des autorités publiques dans les lieux privés sont plus limités que dans les lieux publics. La présente étude n'examine pas les questions juridiques soulevées par la vidéosurveillance des lieux privés, qui concerneraient notamment les banques, les casinos, les magasins et les lieux de résidence privés. Néanmoins, la vidéosurveillance des lieux publics peut fortuitement toucher des lieux privés et constituer, par exemple, une intrusion visuelle dans les foyers par les autorités.

11. La sphère privée recouvre l'aspect intime de la personnalité d'un être humain. Elle suppose le droit pour chacun d'être protégé contre l'ingérence injustifiée des services de l'État, des médias et de toute autre personne physique ou morale. La vie privée est donc une sphère très large qui n'est pas facile à définir : elle ne se limite pas à un « cercle intime » au sein duquel la personne peut mener sa propre vie privée. La sphère privée comprend le droit d'établir et d'entretenir des relations avec d'autres êtres humains, notamment dans le domaine affectif, pour le développement et l'accomplissement de sa propre personnalité[1]. La vie privée concerne également l'intégrité physique et morale d'une personne, y compris sa vie sexuelle.

---

[1] Commission européenne des droits de l'Homme, *X c. Islande*, décision of 18 juillet 1976, pp. 86-87 ; CouDH, *Klass et autres c. Allemagne*, arrêt du 6 septembre 1978 ; CouDH, *Leander c. Suède*, arrêt du 26 mars 1987. La CouDH a fait une synthèse de sa jurisprudence 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* : « La « vie privée » est une notion large, qui ne se prête pas à une définition exhaustive. La Cour a déjà déclaré que des facteurs tels que l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle sont des éléments importants de la sphère personnelle protégée par l'article 8 (voir, par exemple, arrêts *B. c. France*, 25 mars 1992, série A n° 232-C, pp. 53-54, § 63 ; *Burghartz c. Suisse*, 22 février 1994, série A n° 280-B, p. 28, § 24 ; *Dudgeon c. Royaume-Uni*, 22 octobre 1981, série A n° 45, pp. 18-19, § 41 ; et *Laskey, Jaggard et Brown c. Royaume-Uni*, 19 février 1997, *Recueil* 1997-I, p. 131, § 36). L'article 8 protège également le droit à l'identité et au développement personnel ainsi que le droit pour tout individu de nouer et développer des relations avec ses semblables et le monde extérieur (voir, par exemple, *Burghartz*, arrêt précité, avis de la Commission, p. 37, § 47 ; *Friedl c. Autriche*, arrêt du 31 janvier 1995, série A n° 305-B, avis de la Commission, p. 20, § 45). Il peut s'étendre à des activités professionnelles ou commerciales (arrêt *Niemietz c. Allemagne*, 16 décembre 1992, série A n° 251-B, pp. 33-34, § 29 ; et arrêt *Halford* précité, p. 1016, §§ 44, 56) ».

12. D'autres droits fondamentaux, tels que la liberté de pensée, de conscience et de religion, relèvent eux aussi de la sphère de la vie privée, que ce soit au titre de l'article 18 du PIDCP[2] ou de l'article 9 de la CEDH[3].

5. Vidéosurveillance

13. La vidéosurveillance est un système technologique de surveillance au moyen de caméras qui peut être retenu, mis en place et utilisé par les autorités publiques dans des lieux publics aux fins de la prévention, voire de la répression, des infractions. Ce dispositif comporte généralement plusieurs caméras vidéo reliées en télévision de circuit fermé (TVCF). Les images sont envoyées vers un moniteur central de télévision et/ou enregistrées. Le plus souvent, une installation de TVCF comprend plusieurs caméras reliées à une salle de contrôle dans laquelle des opérateurs visualisent une rangée d'écrans de télévision. Le système de TVCF nécessite donc l'intervention d'un être humain pour visualiser les moniteurs ou visionner l'enregistrement.

14. La présente étude ne concerne pas les systèmes vidéo qui reconnaissent automatiquement les plaques d'immatriculation des véhicules en mouvement, ni les systèmes qui surveillent les flux de la circulation et prennent sur le fait les contrevenants au code de la route.

15. Elle n'examine pas non plus les questions juridiques que peut soulever l'utilisation de fausses caméras ou de faux outils de surveillance vidéo, ni ses conséquences, car, s'ils peuvent avoir le même objectif préventif que les systèmes fonctionnels aux fins du maintien de l'ordre public, ces dispositifs posent particulièrement problème non pas sur le plan des droits de l'homme, mais en matière de responsabilité.

16. La présente étude vise les systèmes de vidéosurveillance ou de TVCF – les deux expressions y sont employées indistinctement – utilisés dans les lieux publics ou comme mode de prévention ou de répression des troubles à l'ordre public en général ou des infractions graves en particulier. Il faut ajouter que la TVCF a officiellement pour but de défendre, renforcer et rétablir la sécurité publique.

---

2 L'article 18 est ainsi libellé :

« 1. Toute personne a droit à la liberté de pensée, de conscience et de religion ; ce droit implique la liberté d'avoir ou d'adopter une religion ou une conviction de son choix, ainsi que la liberté de manifester sa religion ou sa conviction, individuellement ou en commun, tant en public qu'en privé, par le culte et l'accomplissement des rites, les pratiques et l'enseignement.

2. Nul ne subira de contrainte pouvant porter atteinte à sa liberté d'avoir ou d'adopter une religion ou une conviction de son choix.

3. La liberté de manifester sa religion ou ses convictions ne peut faire l'objet que des seules restrictions prévues par la loi et qui sont nécessaires à la protection de la sécurité, de l'ordre et de la santé publique, ou de la morale ou des libertés et droits fondamentaux d'autrui.

4. Les États parties au présent Pacte s'engagent à respecter la liberté des parents et, le cas échéant, des tuteurs légaux de faire assurer l'éducation religieuse et morale de leurs enfants conformément à leurs propres convictions. »

3 L'article 9 de la CEDH est ainsi libellé :

« 1. Toute personne a droit à la liberté de pensée, de conscience et de religion ; ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privé, par le culte, l'enseignement, les pratiques et l'accomplissement des rites.

2. La liberté de manifester sa religion ou ses convictions ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité publique, à la protection de l'ordre, de la santé ou de la morale publiques, ou à la protection des droits et libertés d'autrui. »

17. La vidéosurveillance, à plusieurs égards, est beaucoup plus efficace que l'observation humaine. Tout d'abord, la technologie s'est considérablement améliorée et peut être extrêmement ingénieuse : ainsi, la vision de nuit est possible, les possibilités de zoom et de pistage automatique sont courantes, et certains faits, détails et traits précis qui seraient invisibles ou non visibles à l'œil nu peuvent être détectés. Un dispositif intelligent peut même détecter de fausses barbes ou de fausses moustaches et peut comporter un système de reconnaissance faciale ou vocale. En outre, la possibilité de reproduire la même image sur plusieurs moniteurs pouvant être visualisés par plusieurs observateurs améliore les possibilités de contrôle de certains événements, faits ou comportements qui, autrement, pourraient échapper à l'attention d'un observateur sur le terrain.

18. Outre le perfectionnement des technologies de vidéosurveillance et les progrès continus de la résolution optique, la TVCF élargit également le champ de la surveillance. En effet, l'opérateur qui visualise les moniteurs de la TVCF peut surveiller simultanément des images émanant de plusieurs dispositifs d'enregistrement placés à divers endroits. Il devient ainsi plus facile d'observer de manière envahissante et permanente les personnes et les lieux ; le champ de vision, par rapport à l'observation humaine, s'en trouve élargi.

19. Lorsque l'on est observé par un être humain, on peut adapter son comportement et, au bout du compte, se conduire d'une manière plus « conformiste » ; au contraire, un système de TVCF peut être invisible au public et l'existence ainsi que l'identité du contrôleur sont en général inconnues de lui. Le public ne se rend donc pas compte de l'existence d'un contrôleur, ni même de son identité.

20. Enfin, autre point important concernant la vidéosurveillance par rapport à l'observation humaine, de nombreux systèmes de TVCF disposent de systèmes d'enregistrement permettant l'enregistrement et la conservation de toutes les images ou de celles sélectionnées par le contrôleur. En revanche, la configuration de ces systèmes peut varier, en ce que les images rassemblées peuvent même être utilisées abusivement ou diffusées sur l'Internet en direct ou en différé.

21. En conclusion, si l'on compare la vidéosurveillance à l'observation humaine en l'état actuel des choses, il devient évident que la TVCF offre bien plus de possibilités et pourrait donc être bien plus attentatoire aux droits de l'homme que l'observation humaine.

II. Analyse juridique

22. La vidéosurveillance des lieux publics touche plusieurs droits individuels protégés à l'échelon tant international que national. Par ailleurs, la TVCF soulève certaines questions ayant trait à la protection des données à caractère personnel.

A. Quels droits fondamentaux sont en jeu ?

1. Le droit à la vie privée

a. La vie privée sur le plan international

23. Le droit à la vie privée est protégé par des instruments internationaux tels que le Pacte international sur les droits civils et politiques (PIDCP), en son article 17[4], et par la Convention européenne des droits de l'homme (CEDH), en son article 8[5].

[4] L'article 17 du PIDCP est libellé ainsi :

« 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

24. Le fait qu'une personne pénètre dans un lieu public ou y demeure implique que celle-ci est consciente qu'elle sera au moins vue, sinon reconnue, et que son comportement pourra être observé par autrui au sein de cette sphère publique. Elle peut donc en tirer ses propres conclusions et décider d'adapter son comportement en conséquence. 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.

25. Si une personne qui se rend dans un lieu public peut très bien penser que sa vie privée sera moins protégée, elle ne s'attend pas et ne doit pas s'attendre à être privée de ses droits et libertés, y compris ceux se rapportant à sa sphère privée et à son image (voir § 10-12).

26. La plupart des affaires ayant trait à la protection du droit à la vie privée portent sur des violations alléguées de ce droit dans des lieux non publics ou par des moyens autres que la vidéosurveillance. Cela ne veut pas dire pour autant que la vie privée n'est protégée que dans les lieux privés. En effet, la Cour européenne des droits de l'homme (CouDH) a jugé qu'il existait une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la « vie privée »[6].

27. La CouDH a également estimé qu'« [u]n certain nombre d'éléments entr[ai]ent en ligne de compte lorsqu'il s'agi[ssai]t de déterminer si la vie privée d'une personne [était] touchée par des mesures prises en dehors de son domicile ou de ses locaux privés. Puisqu'à certaines occasions les gens se livrent sciemment ou intentionnellement à des activités qui sont ou peuvent être enregistrées ou rapportées publiquement, ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un facteur significatif, quoique pas nécessairement décisif. Une personne marchant dans la rue sera forcément vue par toute autre personne qui s'y trouve aussi. Le fait d'observer cette scène publique par des moyens techniques (par exemple un agent de sécurité exerçant une surveillance au moyen d'un système de télévision en circuit fermé) revêt un caractère similaire. En revanche, la création d'un enregistrement systématique ou permanent de tels éléments appartenant au domaine public peut donner lieu à des considérations liées à la vie privée »[7].

28. Des questions ayant trait au respect de la vie privée peuvent également se poser lorsque des photographies sont prises par la police pendant une manifestation dans un lieu public. Cette ingérence ne sera pas considérée comme une intrusion tant que les données rassemblées ne sortiront pas d'un dossier administratif et ne seront pas transférées dans un système de gestion de données afin d'identifier les personnes[8].

---

2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

5 L'article 8 CEDH est libellé ainsi :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

6 CouEDH, *P.G. et J.H. c. Royaume-Uni*, arrêt du 6 février 2001, § 56.

7 *Ibidem*, § 57.

8 *Ibidem*, § 58.

29. 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, qui peuvent constituer une atteinte illicite au droit à la vie privée, surtout si les données ont été rassemblées par des méthodes cachées de surveillance[9].

30. Des problèmes particuliers se posent lorsque les données rassemblées sont utilisées abusivement. À cet égard, la CouDH, dans l'arrêt *Peck c. Royaume-Uni*, a estimé que la publication ou la divulgation générale, par exemple à des fins de télédiffusion, de données obtenues grâce à des caméras de TVCF constituaient une intrusion dans la vie privée, alors même que les faits sur lesquels l'attention du public était attirée s'étaient produits en public[10].

31. L'affaire *Peck* mérite que l'on expose l'ensemble de ses circonstances car elles sont particulièrement pertinentes au regard des questions examinées dans la présente étude. Un homme atteint d'une dépression marchait seul dans la rue avec un couteau de cuisine dans la main et a tenté de se suicider. Il ignorait qu'il était filmé par une caméra de TVCF installée par les autorités locales. L'opérateur de la caméra a prévenu la police, qui est arrivée sur les lieux. Celle-ci s'est emparée du couteau et a incarcéré l'homme, soupçonné d'aliénation mentale, avant finalement de le remettre en liberté. Par la suite, des photographies prises à partir des images de la TVCF ont été publiées, donnant une image positive de l'utilisation par la police de la surveillance par TVCF. Le matériau rassemblé à cette occasion a ensuite été utilisé par plusieurs médias, qui n'ont fait pratiquement aucun effort pour dissimuler le visage du requérant. La CouDH a relevé que, après la diffusion des images de la TVCF, la scène en question 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 excédait ce que le requérant aurait pu prévoir. La diffusion par le conseil municipal des images en question constituait donc une ingérence grave dans l'exercice du droit au respect de la vie privée du requérant.

32. Le droit à la vie privée, qui se rapporte à la dignité des personnes, protège celles-ci à tout moment et quel que soit le lieu. Le simple fait d'observer l'apparence d'une personne et son comportement dans des circonstances normales posera de graves problèmes si le but visé est susceptible de porter atteinte à la vie privée, à l'honneur et à la dignité de cette personne.

33. Bien que les données à caractère personnel relèvent elles aussi du domaine de la vie privée, le droit à la protection de celles-ci sera analysé plus avant aux paragraphes 38 à 46 ci-après.

b. La vie privée sur le plan national

34. Le droit à la vie privée est expressément protégé au niveau constitutionnel dans la quasi-totalité des États membres du Conseil de l'Europe (CdE)[11]. Aussi les cours constitutionnelles ou les juridictions à compétence équivalente peuvent-elles fonder leurs décisions en matière de protection de la vie privée non seulement sur l'interprétation des instruments internationaux ayant force obligatoire donnée par les juridictions internationales, mais aussi sur leur propre constitution.

---

9 CouEDH, *Amann c. Suisse*, arrêt du 16 février 2000, § 65-66.

10 CouEDH, *Peck c. Royaume-Uni*, arrêt du 28 janvier 2003, § 44.

11 Voir par exemple dans CODICES la Constitution des pays suivants: Andorre (art. 13-14), Arménie (art. 20 -21), Autriche (art. 10), Azerbaïdjan (art. 32), Belgique (art. 22), Bosnie-Herzégovine (art. 3), Bulgarie (art. 32), Croatie (art. 35), Chypre (art. 15), Finlande (section 10), Géorgie (art. 20), Grèce (art. 9), Islande (art. 71), Irlande (art. 40, 42, 44 et 45), Lettonie (art. 96), Lituanie (art. 22), Malte (art. 32), Moldova (art. 28), Pays-Bas (art. 10), Pologne (art. 30-31), Portugal (art. 26), Roumanie (art. 26), Fédération de Russie (art. 23), République slovaque (art. 19-21), République slovène (art. 35), Espagne (art. 18), Suède (Chap. I, art. 2), Suisse (art. 13), « l'ex-République yougoslave de Macédoine » (art. 25), Turquie (art. 20), Ukraine (art. 32).

35. S'agissant du droit à la vie privée dans le contexte de la vidéosurveillance, les juridictions nationales, dans certaines décisions, ont analysé la licéité de ce procédé au regard du droit constitutionnel à la vie privée. Ainsi, le Tribunal constitutionnel du Portugal, dans sa décision n° 225/2202, a dit que « l'utilisation de systèmes de surveillance électronique et la surveillance des particuliers par des organes privés de sécurité constitu[aient] une limitation ou une restriction du droit à la protection de la vie privée, consacré à l'article 26 de la Constitution »[12].

36. En revanche, une affaire tranchée par la Cour constitutionnelle de Hongrie (n° 35/2002[13]), qui statuait sur la constitutionnalité de certaines dispositions de la loi sur le sport, en vertu desquelles les organisateurs d'épreuves sportives devaient recourir à la vidéosurveillance pour assurer la sécurité du public et de ses biens, avait été examinée à l'aune du droit à la protection des données. L'un des juges, dans l'exposé de son opinion concordante, a souligné que la Cour aurait dû examiner les dispositions contestées de la loi sur le sport au regard non pas du droit à la protection des données, mais du droit à la vie privée.

37. Ces éléments peuvent contribuer à démontrer que si la protection des données à caractère personnel relève du domaine de la vie privée, celles-ci bénéficient en outre d'une protection spécifique. Si les deux questions ne sont peut-être pas les mêmes, leur but reste identique.

2. Le droit à la libre circulation

38. La vidéosurveillance dans les lieux publics touche également le droit à la libre circulation des personnes se trouvant légalement sur le territoire d'un État. Le droit à la libre circulation est énoncé à l'article 2 du Protocole additionnel n° 4 à la CEDH[14]. Cette liberté concerne non seulement le droit de circuler librement dans un espace concret, mais aussi le droit de se déplacer sans être constamment suivi[15].

3. La protection des données

39. Étant donné que la vidéosurveillance peut donner lieu à une opération de traitement des données à caractère personnel (c'est-à-dire lorsqu'elles sont rassemblées), le droit à la protection de ces données est concerné lui aussi.

40. Le cadre juridique de la protection des données vise à garantir que celles-ci soient traitées dans le respect non seulement de la vie privée, mais aussi des libertés et droits fondamentaux.

---

[12] Tiré du Document WP89, n° 4/2004, adopté le 11 février 2004, note de bas de page 5. (www.europa.eu.int/privacy).

[13] Voir dans CODICES : HUN-2002-2-003 a) Hongrie / b) Cour constitutionnelle / c) / d) 19-07-2002 / e) 35/2002 / f) / g) Magyar Közlöny (journal officiel), 2002/100 / h).

[14] L'article 2 est libellé ainsi :

> « 1. Quiconque se trouve régulièrement sur le territoire d'un Etat a le droit d'y circuler librement et d'y choisir librement sa résidence.
>
> 2. Toute personne est libre de quitter n'importe quel pays, y compris le sien.
>
> 3. L'exercice de ces droits ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à la sûreté publique, au maintien de l'ordre public, à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui..
>
> 4. Les droits reconnus au paragraphe 1er peuvent également, dans certaines zones déterminées, faire l'objet de restrictions qui, prévues par la loi, sont justifiées par l'intérêt public dans une société démocratique. »

[15] Ainsi, le fait d'exiger d'une personne qu'elle porte une ceinture électronique comme mesure alternative à la détention est considéré comme une atteinte à sa liberté personnelle.

a. La protection des données sur le plan international

41. Comme il a déjà été indiqué, la protection des données personnelles relève du domaine de la vie privée au sens de l'article 8 de la CEDH.

42. La vidéosurveillance relève aussi du champ d'application de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108), entrée en vigueur le 1er octobre 1985. Cette convention a pour but de protéger les personnes[16] contre les abus auxquels peuvent donner lieu le rassemblement et le traitement des données à caractère personnel[17], et de réglementer par la même occasion les flux transfrontières des données à caractère personnel, par exemple celles rassemblées au moyen de caméras vidéo et diffusées en direct, même lorsqu'elles ne sont pas enregistrées.

43. La vidéosurveillance relève du champ d'application de cette Convention dans la mesure où les données tirées des sons et des images concernent des individus qui sont ou peuvent être identifiés en les rattachant à d'autres données, par exemple des mots prononcés, des images statiques ou dynamiques ou d'autres données acoustiques.

44. La Convention consacre également le droit pour toute personne de savoir que des données la concernant sont conservées et, s'il y a lieu, de les faire corriger. Outre le Monténégro, trente-trois États membres du Conseil de l'Europe ont ratifié cette convention.[18]

45. Un Protocole additionnel (STCE n° 181)[19] à la Convention susmentionnée est entré en vigueur le 1er juillet 2004. Ce traité renforce la protection des données à caractère personnel et du droit à la vie privée en apportant des améliorations à la Convention initiale de 1981 sur deux points. Tout d'abord, le protocole prévoit la création d'autorités nationales de contrôle chargées de veiller au respect des lois et règlements adoptés en application de la Convention en matière

---

16 L'article 1er de la Convention est libellé ainsi :

« Article 1er – Objet et but

Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ("protection des données"). »

17 « Article 2 – Définitions

Aux fins de la présente Convention:

a. « données à caractère personnel » signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»);

b. « fichier automatisé » signifie: tout ensemble d'informations faisant l'objet d'un traitement automatisé;

c. « traitement automatisé » s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion;

d. « maître du fichier » signifie: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées. »

18 Albanie, Autriche, Belgique, Bosnie-Herzégovine, Bulgarie, Croatie, Chypre, République tchèque, Danemark, Estonie, Finlande, France, Géorgie, Allemagne, Grèce, Hongrie, Islande, Irlande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Serbie, Slovaquie, Slovénie, Espagne, Suède, Suisse, « Ex-République yougoslave de Macédoine », Royaume-Uni.

19 Intitulé complet : « Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données ».

de protection des données à caractère personnel et de flux transfrontières de données. La seconde amélioration concerne les flux transfrontières de données vers les pays tiers. Les données ne peuvent être transférées que si les États ou les organisations internationales destinataires assurent un niveau de protection adéquat. Ce Protocole a été ratifié par quinze pays du Conseil de l'Europe[20].

46. La directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel n'entre pas dans le champ de la présente étude car ce texte ne s'applique pas au traitement des données audiovisuelles dans un but se rapportant au maintien de l'ordre public, à la prévention des infractions pénales ou à la lutte contre le crime dans les lieux publics.

b. La protection des données sur le plan national

47. Les données à caractère personnel sont protégées sur le plan constitutionnel dans certains pays[21].

48. De nombreux pays, notamment ceux qui ont ratifié les conventions internationales susmentionnées [22], ont adopté des lois expresses en la matière.

B. Licéité des restrictions à l'exercice des droits susmentionnés

1. Conditions posées par le droit international

49. La vidéosurveillance des lieux publics peut conduire à des restrictions du droit au respect de la vie privée, du droit à la liberté de circulation ou du droit à la protection des données à caractère personnel. Cette opération doit donc être exercée conformément aux prescriptions du PIDCP, c'est-à-dire qu'il faut donc établir qu'elle est « légale » et non pas « arbitraire » et, plus particulièrement, qu'elle est justifiée au regard des conditions posées par l'article 8, paragraphe 2, de la CEDH :

> « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

50. Les réglementations nationales ou les autorités publiques qui entendent mettre en place et utiliser des technologies vidéo afin d'observer des lieux publics par vidéosurveillance devront se conformer à ces conditions expresses qui vont être analysées plus avant.

---

[20] Albanie, Bosnie-Herzégovine, Croatie, Chypre, République tchèque, Allemagne, Hongrie, Lituanie, Luxembourg, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Suède.

[21] Voir par exemple dans CODICES les constitutions des pays suivants: Albanie (art. 35), Arménie (art. 20), Azerbaïdjan (art. 32), Belgique (art. 22), Finlande (section 10), Géorgie (art. 20), Croatie (art. 37), Estonie (art. 42), Pays-Bas (art. 10), Pologne (art. 51), Portugal (art. 35), Suède (Chap. II, art. 3), « Ex-République yougoslave de Macédoine » (art. 18),

[22] Pour un aperçu général du droit national en matière de protection des informations et de ses dispositions principales, voir la tableau à l'adresse Internet suivante :http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/legislations_nationales/LegislationsNationales_fr.asp#TopOfPage.

a. Les restrictions doivent être prescrites par la loi

51. Bien que certaines constitutions nationales[23] ou que la version française de l'article 8, paragraphe 2, de la CEDH et de l'article 2, paragraphe 3, du Protocole n° 4 disposent que les restrictions doivent être « prévue[s] par la loi », la CouDH a jugé que l'article 8, paragraphe 2, de la CEDH n'exigeait pas comme base juridique un acte émanant formellement du législateur. Un texte réglementaire ou une règle de droit international peuvent eux aussi constituer une base suffisante[24], de même qu'une règle non écrite tirée par exemple de la *common law*[25].

52. Toutefois, la CouDH a établi des critères assez stricts en ce qui concerne la qualité de la base juridique permettant l'ingérence dans l'exercice des droits protégés :

53. **a.a.** La base juridique doit être accessible au public : cela signifie que « le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné »[26]. Cela revient à poser comme principe que l'individu est censé connaître la base juridique, au moins grâce au concours d'un expert en droit.

54. **a.b.** La base juridique doit être libellée de manière suffisamment précise afin que le public puisse en déterminer précisément à l'avance la portée et le sens de manière à lui permettre d'adapter et de régler sa conduite et son comportement. Un citoyen, « en s'entourant au besoin de conseils éclairés, … doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »[27].

55. **a.c.** Des garanties suffisantes contre les abus doivent être prévues selon des modalités permettant de délimiter avec suffisamment de netteté l'étendue du pouvoir d'appréciation des autorités et de définir les circonstances dans lesquelles celui-ci doit être exercé « compte tenu du but légitime poursuivi, pour fournir à l'individu une protection adéquate contre l'arbitraire »[28]. Cette condition rattache le principe de légalité à celui de l'État de droit et revêt une importance particulière lorsque la surveillance est effectuée aléatoirement.

56. Il ressort de ces observations que les autorités nationales, y compris les juridictions, lorsqu'elles examinent la compatibilité d'une opération de vidéosurveillance avec les dispositions de la Convention, doivent accorder une attention particulière à la qualité de sa base juridique.

---

23 Voir par exemple l'article 10 de la constitution néerlandaise « …sauf restrictions à établir par la loi ou en vertu de la loi… »

24 CouEDH, *De Wilde, Ooms et Versyp c. Belgique*, arrêt du 18 juin 1971, § 93.

25 CouEDH, *Sunday Times c. Royaume-Uni*, arrêt du 26 avril 1979, § 47 et 49.

26 CouEDH, *Sunday Times c. Royaume-Uni*, arrêt du 26 avril 1979, § 47 et 49. Pour que la règle soit accessible, il n'est pas nécessaire qu'elle soit codifiée.

27 CouEDH, *Landvreugd c. Pays-Bas*, arrêt du 4 juin 2002, § 54.

28 CouEDH, *Olsson c. Suède*, arrêt du 24 mars 1988, § 61.

b. Les restrictions doivent être nécessaires dans l'une société démocratique

57. La CouDH a constamment jugé que l'adjectif « nécessaire » n'était pas synonyme d'« indispensable », mais n'était pas non plus aussi souple que des expressions telles qu'« acceptable », « ordinaire », « utile », « raisonnable » ou « souhaitable ». L'ingérence doit correspondre à un « besoin social impérieux » et être « proportionnée au but légitime poursuivi »[29].

58. Cela revient également à poser comme condition que les motifs avancés par les autorités pour justifier l'ingérence doivent être à la fois « pertinents et suffisants »[30].

59. En outre, les mesures qui constituent une ingérence ne doivent pas être telles qu'elles auraient pour effet de décourager l'exercice de droits fondamentaux ou d'autres comportements légitimes[31].

60. En conséquence, les autorités publiques responsables de ces ingérences dans la vie privée des personnes doivent prouver non seulement qu'elles peuvent agir ainsi en vertu d'une base juridique suffisante et adéquate, mais aussi que ce pouvoir, dans les circonstances de la cause, satisfait au critère de nécessité. Même si les autorités nationales jouissent d'une certaine marge d'appréciation, celle-ci est elle aussi soumise en dernier ressort au contrôle de la CouDH.

c. Les restrictions doivent être nécessaires notamment à la sécurité nationale, à la défense de l'ordre ou à la prévention des infractions pénales

61. Les autorités nationales et locales sont mieux placées que la CouDH pour déterminer quelles mesures sont nécessaires pour empêcher les troubles et rétablir l'ordre, prévenir et réprimer les infractions et protéger la sécurité nationale.

62. Elles jouissent donc d'une marge d'appréciation étendue. Dans l'affaire *Leander*, la CouDH a dit : « [p]our préserver la sécurité nationale, les États contractants ont indéniablement besoin de lois qui habilitent les autorités internes compétentes à recueillir et à mémoriser dans des fichiers secrets des renseignements sur des personnes, puis à les utiliser quand il s'agit d'évaluer l'aptitude de candidats à des postes importants du point de vue de ladite sécurité … Vu sa grande marge d'appréciation, le gouvernement défendeur était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant »[32].

63. Pour ce qui est de satisfaire à la condition expresse de la nécessité dans une société démocratique, bien qu'il incombe en premier chef aux autorités nationales de déterminer ce qui est nécessaire pour prévenir les troubles à l'ordre public et les infractions et protéger la sécurité nationale, la CouDH peut également contrôler en dernier ressort le respect de ces conditions.

---

29 CouEDH, *Landvreugd c. Pays-Bas*, arrêt du 4 juin 2002, § 74.

30 CouEDH, *Olsson c. Suède*, arrêt du 24 mars 1988, § 68.

31 CouEDH, *Goodwin c. Royaume-Uni*, arrêt du 27 mars 1996, § 39.

32 CouEDH, *Leander c. Suède*, arrêt du 26 mars 1987, § 67.

d. Proportionnalité

64. Les mesures prises et utilisées par les autorités publiques, pour qu'elles soient justifiées, doivent être adaptées au but poursuivi.

65. Une mesure disproportionnée consisterait par exemple à utiliser des systèmes de vidéosurveillance dans les toilettes publiques pour contrôler et faire respecter une politique d'interdiction du tabac en ces lieux.

66. La condition de proportionnalité impose que l'on examine si des mesures de moindre ampleur (moins attentatoires à la vie privée) peuvent être imposées et si elles sont suffisamment efficaces pour accomplir le même but, en l'occurrence la surveillance policière. Ainsi, l'objectif de la prévention de la délinquance ne saurait justifier, sauf dans des cas exceptionnels de menace imminente pour la sécurité ou de risque de crime grave, un système de surveillance non sélectif donnant lieu à des atteintes considérables au droit à la vie privée et à la liberté de circulation du grand public, car on peut penser que des méthodes de surveillance plus sélectives et suffisamment efficaces peuvent être utilisées.

67. Une mesure de surveillance n'est pas davantage justifiée si elle est conçue et/ou utilisée de manière discriminatoire, par exemple afin de recenser uniquement le comportement criminel de certaines parties de la population choisies en fonction de critères spécifiques tels que le sexe ou l'appartenance à un groupe ethnique, une minorité ethnique ou un groupe religieux déterminés, etc. Rassembler des données de ce type ne pourrait être admis qu'à des fins d'identification.

2. Conditions posées par le droit national

68. Les réglementations d'un pays ne peuvent en aucun cas réduire le niveau de protection offert par la CEDH ou par les autres instruments internationaux ratifiés par ce pays.

69. Comme il a déjà été exposé, dans le domaine de la protection des données, de nombreux pays ont non seulement ratifié les conventions du Conseil de l'Europe, mais aussi adopté des lois expresses en la matière.

70. En outre, dans le cadre de la transposition de la Directive 95/46/CE de l'UE relative au traitement des données à caractère personnel obtenues par vidéosurveillance, certains États membres de l'UE ont adopté une législation ou adapté leur réglementation pour se mettre en conformité avec la Directive. Bien que la vidéosurveillance par les autorités publiques ne relève pas expressément du champ d'application de cette directive, des progrès considérables ont été accomplis par la suite en matière de protection des droits individuels, et plus particulièrement dans le domaine de la protection des données[33].

---

[33] Aux termes de l'art. 6 de la Directive, les données à caractère personnel doivent être :

- traitées loyalement et licitement;
- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement;
- exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;

71. Certains pays, par exemple les Pays-Bas et la France, ont adopté des réglementations expresses visant l'installation des systèmes de vidéosurveillance dans les lieux publics. La loi française[34] est un exemple de texte posant des conditions strictes : il doit y avoir un impératif de sécurité pour qu'un système de vidéosurveillance puisse être installé dans un lieu public. En vertu de cette loi, les objectifs de sécurité doivent être très précis. L'installation de dispositifs de ce type est subordonnée à l'autorisation du préfet, après avis d'une commission départementale présidée par un magistrat. En ce qui concerne le respect de la vie privée, les systèmes vidéo doivent être installés de telle sorte qu'ils ne permettent pas de visualiser l'intérieur ou l'entrée d'un immeuble d'habitation. Sauf dans le cadre d'une procédure pénale, les enregistrements peuvent être conservés pendant un délai maximal d'un mois. Le public doit être informé de manière claire et permanente de l'existence du système de vidéosurveillance et de l'autorité ou de la personne responsable au regard de la loi.

3. Autres conditions

72. Compte tenu des particularités du traitement, de l'enregistrement et de la diffusion des images obtenues grâce aux systèmes de vidéosurveillance et des possibilités qu'elles offrent, d'autres conditions doivent être satisfaites sur plusieurs points.

a. En ce qui concerne les droits individuels

73. Les gens doivent être prévenus lorsqu'ils sont observés sur les lieux publics ou, à tout le moins, le système de surveillance doit être évident[35]. La signalisation n'est pas seulement une condition protégeant le droit à la vie privée ; elle poursuit également un objectif de prévention, à l'instar de la vidéosurveillance. Il faut notamment bien s'assurer que la personne observée, dans des circonstances normales, en soit apparemment consciente ou qu'elle ait donné son consentement sans ambiguïté à ce sujet[36]. En outre, la personne qui a ou aurait fait l'objet de la surveillance doit disposer d'une voie de recours effective et doit être informée de son existence et de ses modalités d'utilisation[37].

- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement…

L'art. 7 de la Directive prévoit que le traitement de données à caractère personnel ne peut être effectué que si :

- la personne concernée a donné son consentement; ou
- il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée; ou
- subject;
- il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées; ou
- il est nécessaire à la réalisation de l'intérêt légitime poursuivi … à condition que ne prévale pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée ...

[34] Loi n° 95-73 du 21 janvier 1995 et décret n° 96-926 du 17 octobre 1996.

[35] La signalisation des systèmes de vidéosurveillance peut se faire au moyen de panneaux placés à des endroits appropriés dans la rue ou, à tout le moins, en s'assurant par tout autre moyen que le public est informé que certains lieux publics font l'objet d'une surveillance.

[36] Même une personne en détention, qui peut s'attendre à ce que son comportement fasse l'objet d'une certaine forme de surveillance, a le droit d'être prévenu si les informations rassemblées au centre de détention seront utilisées dans un but que cette personne n'aurait pas pu prévoir (voir CouEDH, *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, § 42-43).

[37] CouEDH, *Perry c. Royaume-Uni*, arrêt du 17 juillet 2003, § 47-49.

b. En ce qui concerne les données rassemblées grâce à la vidéosurveillance

74. Les données personnelles faisant l'objet d'un traitement automatique minutieux doivent être rassemblées et traitées équitablement et dans le respect de la loi, conservées dans un but précis et légitime et utilisées conformément à celui-ci. Elles doivent être adéquates et pertinentes et ne pas être excessives par rapport au but dans lequel elles sont conservées. Elles doivent être fiables et, s'il y a lieu, mises à jour. Enfin, elles doivent être préservées sous une forme qui permet l'identification des personnes visées par les données pendant un délai d'une durée non excessive au regard du but dans lequel ces données sont conservées.

c. En ce qui concerne l'accès aux données rassemblées

75. Toute personne a le droit d'accéder aux données rassemblées à son sujet. En outre, chacun a le droit d'être prévenu que des données comme celles-ci ont été rassemblées et traitées, qu'elles aient été communiquées ou non à d'autres personnes ou institutions, et d'être informé de l'usage qui en sera fait.

76. En principe, les règles de droit commun concernant le caractère public des données détenues par le gouvernement s'appliquent, sauf s'il existe une législation spéciale.

77. Si et dans la mesure où il nuit à la prévention ou à la répression des infractions, à la protection de la sécurité ou aux droits (à la vie privée) d'autrui, l'accès à ces données peut être restreint. Ainsi, une personne qui aurait besoin d'informations afin de préparer sa défense en cas de poursuites pénales disposerait d'arguments solides pour accéder à ces informations en vertu de son droit à un procès équitable dans l'égalité des armes. Mais, même dans cette hypothèse, il faut mettre en balance l'ensemble des intérêts concernés, y compris ceux des tiers.

78. Enfin, les mesures de vidéosurveillance doivent être contrôlées par une autorité indépendante. Ainsi, aux Pays-Bas, une Commission de protection des données à caractère personnel a été créée par la loi, et toute opération de rassemblement et de traitement de données à caractère personnel visée par la loi est contrôlée par cette Commission, tandis que celle-ci doit être informée de toute opération de ce type non visée par la loi.

III. Conclusions et recommandations

79. La vidéosurveillance des lieux publics par les autorités publiques ou les services répressifs peut constituer une menace indéniable pour des droits fondamentaux tels que le droit à l'intimité et au respect de la vie privée, du domicile et de la correspondance, le droit à la liberté de circulation et le droit à ce que les données à caractère personnel rassemblées par ce moyen bénéficient d'une protection spécifique.

80. Dans les lieux publics, les individus doivent s'attendre à ce que leur droit à la vie privée soit moins protégé, ce qui ne signifie pas pour autant qu'ils renoncent à ce droit fondamental.

81. La TVCF étant particulièrement perfectionnée, il est recommandé d'adopter des réglementations expresses à l'échelon tant international que national afin de régir la question particulière de la vidéosurveillance des lieux publics par les autorités publiques en tant que mesure restreignant le droit à vie privée.

82. Il y a lieu, dans ces réglementations, de tenir compte en priorité des éléments suivants :

- Une opération de vidéosurveillance menée compte tenu d'impératifs de sécurité ou de sûreté, ou dans le cadre de la prévention et de la lutte contre la criminalité, doit respecter les conditions énoncées à l'article 8 de la CEDH.

- En ce qui concerne la protection des personnes lorsque des données à caractère personnel sont rassemblées et traitées, les réglementations doivent, à tout le moins, suivre *mutatis mutandis* les conditions posées par la Directive 95/46/CE, notamment en ses articles 6[38] et 7[39], qui reprennent l'article 5 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[40].

83. Par ailleurs, compte tenu des particularités de la vidéosurveillance dans les lieux publics, la Commission recommande de prendre systématiquement les mesures suivantes :

---

38 Aux termes de l'art. 6 de la Directive, les données à caractère personnel doivent être :

- traitées loyalement et licitement;
- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement;
- exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement…

39 L'art. 7 prévoit que le traitement de données à caractère personnel ne peut être effectué que si :

- la personne concernée a donné son consentement; ou
- il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée; ou
- subject;
- il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées; ou
- il est nécessaire à la réalisation de l'intérêt légitime poursuivi … à condition que ne prévale pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée ...

40 L'article 5 de la Convention est libellé ainsi :

« Article 5 – Qualité des données

Les données à caractère personnel faisant l'objet d'un traitement automatisé sont:

a. obtenues et traitées loyalement et licitement;

b. enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;

c. adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;

d. exactes et si nécessaire mises à jour;

e. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. »

- Les gens doivent être prévenus qu'ils sont surveillés dans les lieux publics, sauf si le système de surveillance est évident. Cela signifie que, concrètement, on pourra présumer que la personne observée est consciente qu'elle fait l'objet d'une surveillance ou qu'elle a donné son consentement sans ambiguïté à ce sujet.

- Une autorité indépendante spécialisée doit être mise en place, comme l'ont fait plusieurs États européens[41], afin de garantir le respect des conditions prévues par le droit interne donnant effet aux principes et prescriptions du droit international en matière de protection des individus et des données à caractère personnel.

[41] France, Italie, Pays-Bas.