Strasbourg, le 8 juin 2007

CDL-AD(2007)027

Etude n° 430 / 2007

Or. angl.

COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT
(COMMISSION DE VENISE)

AVIS

SUR LA VIDÉOSURVEILLANCE DANS LES SPHERES PUBLIQUES ET PRIVÉES PAR DES OPÉRATEURS PRIVÉS ET DANS LA SPHERE PRIVÉE PAR LES AUTORITÉS PUBLIQUES ET LA PROTECTION DES DROITS DE L'HOMME

Adopté par la Commission de Venise
lors de sa 71e session plénière
(Venise, 1er - 2 juin 2007)

sur la base des observations de

M. Pieter van DIJK (membre, Pays-Bas)
M. Vojin DIMITRIJEVIC (membre, Serbie)

I. *Introduction*

1. *La Commission de Venise a adopté à sa 70e session plénière (16-17 mars 2007) un « Avis sur la vidéosurveillance dans les lieux publics par les autorités publiques et la protection des droits de l'homme » (CDL-AD(2007)014). Cet avis faisait suite à une lettre du président de la commission des questions juridiques et des droits de l'homme, M. Dick Marty, datée du 10 octobre 2006, dans laquelle celui-ci demandait l'avis de la Commission de Venise sur la question de savoir dans quelle mesure la vidéosurveillance était compatible avec les droits fondamentaux de l'homme dans le cadre de l'élaboration du rapport sur « La vidéosurveillance dans les lieux publics ».*

2. *Pour se rendre parfaitement compte de l'évolution actuelle des activités de vidéosurveillance, et ne pas s'attacher exclusivement aux dangers des activités de vidéosurveillance menées par les autorités publiques, la Commission de Venise a décidé d'étendre son analyse à la vidéosurveillance par des opérateurs privés dans les sphères publique et privée et à la vidéosurveillance par les autorités publiques dans la sphère privée.*

3. *En effet, sur le plan privé, les gens utilisent de plus en plus du matériel de vidéosurveillance pour savoir ce qui se passe chez eux et à l'extérieur de leur domicile. L'utilisation de dispositifs de vidéosurveillance a augmenté au fil des années que ce soit à domicile avec ce qu'il est convenu d'appeler les « nounou-cams », ou qu'il s'agisse de l'utilisation plus classique d'une caméra installée à l'entrée d'une maison ou d'une propriété privée plus vaste. De plus, en raison des progrès technologiques, la baisse du coût des dispositifs de vidéosurveillance a entraîné une augmentation de l'utilisation parmi le public.*

4. *La révolution qu'a été Internet a en outre eu des incidences profondes sur la vidéosurveillance. Internet a permis d'instituer virtuellement la vidéosurveillance quasiment partout et de faire l'objet d'une surveillance partout dans le monde. Grâce aux satellites qui émettent des signaux dans le monde entier, il est désormais possible de surveiller les gens, où qu'ils se trouvent, à partir d'un ordinateur portable. L'« œil du maître » est devenu une réalité grâce à la vidéo en continu, système à distance qui permet aux particuliers de surveiller leur site par Internet, quel que soit l'endroit où ils se trouvent, car les images sont archivées sur un serveur web à distance. Internet et la propagation de la technologie Wi-Fi ont supprimé quasiment toutes les frontières et permettent d'enregistrer et de visualiser des images vidéo partout dans le monde.*

5. *La présente étude est un pas de plus dans l'examen, par la Commission de Venise, de la question de la vidéosurveillance et des droits de l'homme ; la commission entend définir des principes directeurs pour concilier intérêts publics et droits de l'homme et libertés individuelles dans une société démocratique.*

6. *M. Pieter van Dijk et M. Vojin Dimitrijevic ont été nommés rapporteurs.*

7. *La présente étude, établie sur la base de leurs observations, a été adoptée par la Commission de Venise lors de sa 71e session plénière (Venise, 1er - 2 juin 2007).*

II. Champ de la présente étude

8. La présente étude porte sur l'observation des personnes par des opérateurs privés dans les lieux publics et privés et par les autorités publiques dans les lieux privés 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 ou non enregistrées. Elle examine ces pratiques au regard des normes européennes en matière de droits de l'homme.

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

Opérateurs privés

10. Aux fins de la présente étude, l'expression « opérateurs privés » s'entend de personnes physiques ainsi que des sociétés privées comme les cabinets d'enquête privés, les personnes morales de droit privé comme les casinos, les banques ou les établissements semi-publics ou toute entreprise ou société commerciale.

Autorités publiques

11. Par « autorités publiques », il faut entendre 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.

Sphère publique

12. Un « lieu public » est un endroit auquel quiconque, en principe, peut accéder librement, sans distinction. Il peut être utilisé par tous librement. Les lieux publics sont régis par le droit public et contrôlés par les autorités publiques dont les pouvoirs en matière d'application de la loi et d'intervention y sont plus étendus que dans les lieux privés.

13. A titre d'exemples de lieux publics on peut citer les parcs publics, les rues piétonnes des centres-villes, les parcs de stationnement extérieurs, les rues des quartiers résidentiels, les stades de sport et les stations de métro.

14. Les universités, les hôpitaux, les stades, les bureaux de poste et les établissements scolaires sont des exemples de « lieux semi-publics » auxquels en principe, les règles de la sphère publique s'appliquent aussi.

Sphère privée

15. La « sphère privée », au sens concret, est un domaine dont l'accès peut être restreint par les personnes qu'elle protège. En principe, elle n'est pas librement ouverte au public et n'est pas accessible indifféremment à tous. Les règles qui la régissent relèvent principalement du droit privé et plus précisément du droit au respect de la vie privée. Les pouvoirs des autorités publiques dans les lieux privés sont plus limités que dans les lieux publics.

16. La catégorie des lieux privés ne se limite pas aux résidences privées mais comprend aussi les bureaux, les magasins, les discothèques, les cafés et les restaurants dont le propriétaire, l'utilisateur ou le gérant est responsable de ce qui s'y passe.

17. Les universités, les hôpitaux, les stades, les bureaux de poste et les établissements scolaires, qui peuvent être considérés comme des lieux semi-publics, peuvent aussi être considérés comme relevant de la sphère privée dans la mesure où les directeurs ou administrateurs sont au premier chef responsables de ce qui s'y passe alors que les autorités publiques seraient responsables de la défense de l'ordre et de la prévention des infractions pénales.

18. Aux fins de la présente étude, relèveront aussi de la sphère privée les lieux de travail et l'utilisation de la vidéosurveillance en milieu professionnel, ce qui soulève des problèmes juridiques concernant le droit des employés au respect de leur vie privée.

19. 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'Etat, des médias et de toute autre personne physique ou morale. La vie privée au sens par exemple de l'article 8 de la Convention européenne des Droits de l'Homme (ci-après dénommée la CEDH) est donc une sphère très large qui n'est pas facile à définir ; elle ne se limite pas à un « cercle intime » dans lequel 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, afin de développer sa propre personnalité et de s'épanouir.[1] La vie privée concerne également l'intégrité physique et morale d'une personne, y compris sa vie sexuelle.

20. Il est rappelé que la liberté de pensée, de conscience et de religion relève aussi de la vie privée, au titre de l'article 18 du Pacte international relatif aux droits civils et politiques (ci-après dénommé le PIDCP) ou de l'article 9 de la CEDH.

Vidéosurveillance

21. Si le système de vidéosurveillance mis en place et utilisé par les autorités publiques dans les lieux publics aux fins de la prévention, voire de la répression des infractions, est d'ordinaire un « système de TVCF » (qui comporte des caméras vidéo reliées en télévision en circuit fermé), la vidéosurveillance exercée par des opérateurs privés ou des autorités publiques dans la sphère privée pourrait comprendre divers types de vidéosurveillance.

22. La présente étude porte donc non seulement sur le système de TVCF mais aussi sur les autres possibilités de vidéosurveillance comme les caméras vidéo simples installées à l'entrée d'une habitation ou d'une autre propriété privée, les « nounou-cams » ou les caméras web.

23. Le fait que la vidéosurveillance, par rapport à l'observation humaine, offre bien plus de possibilités et risque donc d'être plus attentatoire aux droits de l'homme, est encore plus évident ici que par rapport à la vidéosurveillance effectuée par les autorités publiques dans les lieux publics.

III. Analyse juridique

A. La protection de la vie privée sur le plan international

24. Le secteur du droit essentiellement concerné par la vidéosurveillance, c'est-à-dire la collecte ouverte ou non d'enregistrements, d'images et d'informations sur des personnes, serait de l'avis général le droit à la vie privée.

---

[1] Commission européenne des Droits de l'Homme, *X c. Islande,* décision du 18 mai 1976, 86.87.

CouEDH, *Klass et autres c. Allemagne*, arrêt du 6 septembre 1978.

CouEDH, *Leander c. Suède*, arrêt du 26 mars 1987. La CouEDH a fait une synthèse de sa jurisprudence dans 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, CouEDH, arrêts *B. c. France*, 25 mars 1992, paragraphe 63 ; *Burghartz c. Suisse*, 22 février 1994, paragraphe 24 ; *Dudgeon c. Royaume-Uni,* 22 octobre 1981, paragraphe 41 ; et *Laskey, Jaggard et Brown c. Royaume-Uni,* 19 février 1997, paragraphe 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 c. Suisse*, et *Friedl c. Autriche*, arrêt du 31 janvier 1995, avis de la Commission). Il peut s'étendre à des activités professionnelles ou commerciales (arrêts *Niemietz c. Allemagne,* 16 décembre 1992, paragraphe 29, et *Halford c. Royaume-Uni,* 25 mai 1997, paragraphes 44 et 56) ».

25. Les dispositions des traités internationaux relatifs aux droits de l'homme applicables dans ce contexte, qui lient tous les Etats membres du Conseil de l'Europe, figurent essentiellement dans le Pacte international relatif aux droits civils et politiques et dans la CEDH.

L'article 17 du PIDCP est libellé comme suit :

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

L'article 8 de la CEDH est libellé comme suit :

« 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 ».

26. Si les organes internationaux de défense des droits de l'homme ont hésité à définir le droit à la vie privée, la notion de vie privée est importante dans l'éventail des valeurs protégées par l'actuel système européen des droits de l'homme.

27. La meilleure stratégie semblerait être de considérer la vie privée comme un ensemble de valeurs relatives à la sphère intime d'une personne, qui se reflètent dans les divers droits et qui ne peuvent faire l'objet d'ingérences ou être réduites que conformément aux principes et règles généraux et particuliers relatifs à l'exercice des droits fondamentaux concernés.

28. La question de savoir si et comment le droit international offre une protection dépend de la nature de l'opérateur qui exerce l'activité de vidéosurveillance.

1. L'activité de vidéosurveillance est le fait d'un opérateur privé (qu'il s'agisse de lieux publics ou privés)

29. Le fait que les normes internationales consacrées dans le PIDCP et la CEDH s'adressent aux Etats et à leurs organismes publics, et non aux particuliers, pourrait être considéré comme un problème.

30. Toutefois, en ce qui concerne le PIDCP, on peut affirmer que rien dans le libellé de l'article 17 du Pacte implique que l'interdiction d'immixtion s'applique uniquement aux autorités de l'Etat. Le paragraphe 1 de cet article est impersonnel et la protection offerte par la loi contre les « immixtions ou atteintes » sous-entend le droit de la victime de compter sur la protection offerte par la loi (c'est-à-dire l'Etat).

31. Un Etat qui n'offrirait pas une telle protection contre les immixtions arbitraires ou illégales pourrait être considéré comme ne respectant pas ses engagements conventionnels, que l'immixtion dans la vie privée soit ou non le fait d'un particulier.

32. Conformément au PIDCP, toute immixtion dans l'exercice du droit à la vie privée ne peut être justifiée que si l'intervention n'est pas « arbitraire ou illégale ».[2]

33. En ce qui concerne la CEDH, toute requête présentée à la Cour européenne des Droits de l'Homme (CouEDH) qui viserait un particulier serait déclarée irrecevable en raison de son incompatibilité avec le principe *ratione personae* de la Convention. En conséquence, seule la responsabilité de l'Etat est en jeu et non celle d'un particulier.

34. Il n'en demeure pas moins que si la Cour européenne des Droits de l'Homme hésite à élaborer une théorie générale définissant dans quelle mesure la Convention devrait aussi s'appliquer aux relations entre particuliers, il est désormais établi par la jurisprudence que la Convention non seulement oblige les autorités des Etats contractants à respecter les droits et les libertés qu'elle consacre mais exige aussi d'eux qu'ils garantissent l'exercice effectif de ces droits et libertés en évitant toute violation ou en y remédiant.

35. Il se peut donc que les Etats contractants aient, ce qu'il est convenu d'appeler, une « obligation positive » d'adopter des mesures législatives et autres dans le domaine des relations entre particuliers[3].

36. Le premier devoir de l'Etat et des autorités publiques en application de l'article 8 de la CEDH est de s'abstenir de s'ingérer dans l'exercice du droit de chacun au respect de sa vie privée. L'Etat devrait toutefois prendre des mesures concrètes pour assurer ou protéger l'exercice des droits conformément à l'article 8.1 de la CEDH.

37. L'effet dit *Drittwirkung* des dispositions de la Convention est aussi pertinent pour la protection du droit au respect de la vie privée au titre de l'article 8 de la CEDH.

38. L'Etat se doit non seulement de s'abstenir de s'ingérer illégalement dans la vie privée du particulier mais aussi d'empêcher autrui de faire de même.

39. Est titulaire au premier chef du droit au respect de la vie privée la personne qui pénètre dans un espace privé ou public et qui s'attendrait légitimement à ne pas être surveillée par une caméra.

40. Cela étant, le droit à la vie privée comprend aussi le droit d'une personne de contrôler l'accès à sa propriété privée et le comportement adopté dans cette propriété. Le droit au respect de la vie privée est donc concerné dans les deux cas.

41. Pour arriver à un équilibre entre l'intérêt public ou privé en cause dans le contrôle et l'intérêt privé qui ne doit pâtir d'aucune ingérence dans la vie privée, il faut trouver un critère de proportionnalité pour savoir si l'ingérence est proportionnelle à l'intérêt/aux intérêts qui doivent être protégés.

42. L'Etat trouvera ce critère au moyen d'une législation et d'une pratique administrative appropriées et d'un contrôle administratif et judiciaire.

---

[2] D'après le Comité des droits de l'homme, « au sens de l'article 17 il n'y a pas que la procédure qui puisse revêtir un caractère arbitraire. Cette question se pose également en ce qui concerne le caractère raisonnable des atteintes aux droits visés dans ce même article et sa compatibilité avec les buts, objets et objectifs du Pacte ». Voir *Canepa c. Canada,* n° 558/1993, paragraphe 11.4.

[3] CouEDH, arrêts *Marckx c. Belgique*, 13 juin 1979, paragraphe 31; *Botta c. Italie*, 24 février 1998, paragraphe 33 ; *Craxi (n° 2) c. Italie*, 17 juillet 2003, paragraphes 73 à 76.

43. La Commission de Venise a déjà réaffirmé dans son étude sur la vidéosurveillance dans les lieux publics par les autorités publiques et la protection des droits de l'homme (CDL-AD(2007)014) qu'une personne a droit à un certain respect de sa vie privée dans un lieu public. En conséquence, lorsqu'une personne pénètre dans un lieu, elle ne s'attend pas, en règle générale, à être surveillée.

44. Il conviendrait par ailleurs de prendre aussi en considération le droit d'une personne de contrôler l'accès à ses biens privés ainsi que les comportements chez elle.

45. L'Etat se trouve donc face à deux atteintes éventuelles au droit au respect de la vie privée et conformément à son obligation positive, il se doit de protéger effectivement les deux aspects de ce droit.

46. En conséquence la surveillance exercée par des opérateurs privés dans des lieux privés ou publics doit aussi être justifiée d'après les critères énoncés à l'article 8.2 de la CEDH.

47. Conformément à l'article 8.2 de la CEDH, une ingérence peut être justifiée si elle est prévue par la loi et 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 des libertés d'autrui.

48. Pour être justifiée, une règle ou une mesure restrictive doit correspondre à un « besoin social impérieux »[4].

49. Concrètement, un particulier peut avoir un intérêt à observer, de manière attentatoire à la vie privée, un lieu public en vue de protéger son bien et/ou d'assurer la sécurité ou uniquement de défendre l'ordre, de prévenir des infractions pénales ou de protéger certains de ses droits. Le principe de proportionnalité exigerait alors que par exemple, le lieu public en question soit contigu à la zone privée que la personne veut protéger. En d'autres termes, la surveillance peut ne couvrir, dans la rue en question, que les abords immédiats, ou peut être mise en place de manière à ne pas couvrir également l'extérieur ou l'intérieur d'autres habitations.

50. Cela étant, le droit du propriétaire ou de l'habitant de protéger sa propriété privée ne signifie pas qu'une personne qui pénètre sur le territoire d'autrui n'a pas le droit au respect de sa vie privée. La personne doit au contraire être informée ou avoir été raisonnablement rendue attentive pour d'autres motifs, à la surveillance ou à la possibilité d'une surveillance ponctuelle. De plus, comme dans le cas de la surveillance des lieux publics par les autorités publiques, la personne concernée a le droit de savoir si des données ont été enregistrées et dans l'affirmative, comment elles seront traitées et quel usage peut en être fait. Pour finir, elle doit pouvoir faire un recours pour vérifier la légalité de la surveillance.

51. La vidéosurveillance effectuée par des opérateurs privés (un propriétaire, un habitant ou le gérant de locaux privés) peut être exigée par les autorités publiques pour défendre l'ordre ou prévenir des infractions pénales, par exemple dans des discothèques ou des stades de football. En pareils cas, le principe de proportionnalité et les autres principes mentionnés ci-dessus s'appliquent.

---

[4] Voir CouEDH, arrêt *Leander c. Suède,* 26 mars 1987, paragraphe 58 ; *Gillow c. Royaume-Uni,* 24 novembre 1984, paragraphe 55 ; *B c. Royaume-Uni,* 8 juillet 1987, paragraphe 61.

52. Pour ce qui est des lieux de travail, la mise en place d'une surveillance vidéo exige que le droit à la vie privée des employés soit respecté.

53. En pareil cas, la surveillance serait d'une manière générale autorisée pour éviter ou déceler des malversations ou des vols de la part d'employés en cas de soupçons fondés. Toutefois, à l'exception de cas d'espèce, l'enregistrement sur bande vidéo ne serait pas autorisé dans des lieux comme les toilettes, les douches, les vestiaires ni les zones fumeurs et les salons des employés où une personne peut compter sur le fait que sa vie privée sera respectée.

54. De plus, la surveillance secrète ne devrait être autorisée, et uniquement sur une base temporaire, que si elle s'impose faute d'autres solutions appropriées.

55. La surveillance sur le lieu de travail ne sera pas proportionnelle si elle a pour unique objet de vérifier qu'une personne fait son travail et comment elle le fait.

56. Sans entrer dans les détails des diverses conventions collectives et autres accords d'entreprises qui pourraient exister dans les Etats membres du Conseil de l'Europe en matière de protection du droit à la vie privée des employés, les employeurs devraient se conformer à des principes directeurs écrits en matière de respect de la vie privée qui offrent suffisamment de garanties et permettent une supervision effective.

57. Pour ce qui est des magasins, la surveillance par caméras peut se justifier pour protéger les biens si cette mesure se révèle nécessaire et proportionnelle. Elle peut aussi se justifier dans certains endroits du magasin pour prévenir et réprimer les vols qualifiés mais de nouveau uniquement si elle est absolument nécessaire.

58. La législation nationale devra définir clairement la base juridique de la surveillance et la nécessité de l'atteinte compte tenu des intérêts protégés.

59. A ce sujet et particulièrement lors de l'évaluation de la proportionnalité de l'atteinte concernée, les juridictions nationales ont un rôle important à jouer.

2. La vidéosurveillance est exercée par une autorité publique dans des lieux privés

60. Comme indiqué aux paragraphes 15 à 20 ci-dessus, la catégorie des lieux privés ne se limite pas aux domiciles privés, bureaux, magasins, restaurants et lieux de travail où le propriétaire, l'usager ou le gérant est au premier chef responsable de ce qui s'y passe. Il faut aussi penser à des lieux comme les stades, les bureaux de postes, les hôpitaux et les établissements scolaires ; lieux où les autorités publiques ont aussi une responsabilité évidente en matière de défense de l'ordre et de prévention des infractions pénales.

61. Les autorités qui installent et exploitent des caméras pour exercer la surveillance nécessaire le font généralement sur la base d'une loi et dans le cadre d'une consultation et d'une coopération avec les particuliers responsables.

62. Toutefois si elles n'obtiennent pas l'autorisation et la coopération nécessaires, elles peuvent, compte tenu de leurs fonctions et responsabilités publiques (essentiellement défense de l'ordre, prévention et répression des infractions pénales) et de leurs pouvoirs connexes, être autorisées, sur la base d'une loi, à pénétrer dans ces lieux privés pour y installer le matériel nécessaire et également pour le faire fonctionner, le cas échéant.

63. Si le lieu privé est un domicile ou un bureau où se trouvent également des documents privés et d'autres effets personnels, la justification de l'ingérence doit être examinée compte tenu des critères de l'article 8.2 de la CEDH. Dans les autres cas, le critère sera celui de la nécessité en application de l'article 1.2 du Protocole n° 1 à la CEDH[5]. En règle générale, seule une surveillance ponctuelle et temporaire de ces lieux privés par les autorités publiques sera nécessaire et proportionnelle.

B. La protection des données traitées sur le plan international

64. La vidéosurveillance pourrait conduire à traiter des données à caractère personnel. Ce traitement de données à caractère personnel relève de la protection de la vie privée au sens de l'article 8 de la CEDH.

65. La vidéosurveillance et le traitement des données réunies relèvent aussi du champ d'application de la « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » du Conseil de l'Europe[6] qui a été ouverte à la signature le 28 janvier 1981 et est entrée en vigueur le 1er octobre 1985. Cette convention a pour but de protéger les personnes[7] contre les abus auxquels peuvent donner lieu le rassemblement et le traitement de données à caractère personnel[8], et de réglementer par la même occasion les flux transfrontières des données à caractère personnel, par exemple les données rassemblées au moyen de caméras vidéo et diffusées en direct, même lorsqu'elles ne sont pas enregistrées.

---

5 L'article 1er est libellé comme suit :

« Article 1 – Protection de la propriété

Toute personne physique ou morale a droit au respect de ses biens. Nul ne peut être privé de sa propriété que pour cause d'utilité publique et dans les conditions prévues par la loi et les principes généraux du droit international.

Les dispositions précédentes ne portent pas atteinte aux droits que possèdent les Etats de mettre en vigueur les lois qu'ils jugent nécessaires pour réglementer l'usage des biens conformément à l'intérêt général ou pour assurer le paiement des impôts ou d'autres contributions ou des amendes ».

6 STE n° 108

7 L'article 1er de la Convention est libellé comme suit :

« 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 ») ».

8 Article 2 – *Définitions*

Aux fins de la présente Convention :

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

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 ».

66. La vidéosurveillance relève du champ d'application de la « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » 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 sonores.

67. La « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » consacre aussi le droit de toute personne de savoir que des données la concernant sont conservées et, s'il y a lieu, de les faire corriger. Trente-huit Etats membres du Conseil de l'Europe ont ratifié cette convention[9].

68. Un Protocole additionnel[10] à la Convention susmentionnée est entré en vigueur le 1er juillet 2004. Il renforce la protection des données à caractère personnel et du droit au respect de la vie privée en apportant des améliorations à la Convention initiale de 1981 sur deux points. Premièrement, il 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 de protection des données à caractère personnel et de flux transfrontières de données. La deuxième amélioration concerne les flux transfrontières de données vers des pays tiers. Les données ne peuvent être transférées que si les Etats ou les organisations internationales destinataires assurent un niveau de protection adéquat. Le Protocole a été ratifié par quinze Etats membres du Conseil de l'Europe[11].

69. La Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[12] est en principe applicable au traitement de données à caractère personnel, y compris des sons et des images relatives aux personnes physiques, comme en cas de vidéosurveillance. La vidéosurveillance ne relève cependant pas du champ d'application de cette directive si elle est effectuée 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 ou si elle est effectuée par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

C. Autre élément légitimant la vidéosurveillance : la question du consentement

70. Pour être valable, le consentement, quelles que soient les conditions dans lesquelles il est exprimé, doit être une « *manifestation de volonté, libre, spécifique et informée* » comme indiqué à l'article 2 h) de la Directive relative à la protection des personnes physiques à l'égard du traitement des données[13].

---

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

10 STE n° 181, 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 »

11 Albanie, Allemagne, Bosnie-herzégovine, Chypre, Croatie, Hongrie, Lituanie, Luxembourg, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Slovaquie, Suède.

12 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; JO L 281, 23.11.1995, p. 31-50.

13 Voir par exemple les documents de travail WP 12 et WP 114 du Groupe de travail ″article 29″ b .

71. aa) Le consentement doit être donné librement. Par consentement « libre », il faut entendre une décision volontaire d'une personne en possession de toutes ses facultés, prise en l'absence de toute coercition, sociale, financière, psychologique ou autre. Tout consentement donné sous la menace de non-traitement ou de traitement de qualité inférieure dans une situation donnée ne saurait être considéré comme « libre ». Le consentement donné par une personne qui n'a pas eu la possibilité de véritablement choisir ou qui a été mise devant le fait accompli ne saurait être considéré comme valable.

72. Le « Groupe de travail ″article 29″ »[14] est d'avis qu'il ne faut recourir au consentement que s'il s'applique strictement au cas où la personne est complètement libre de le donner et a la possibilité d'y renoncer par la suite sans préjudice[15].

73. bb) Le consentement doit être spécifique. Le consentement « spécifique » doit renvoyer à une situation bien définie et concrète dans laquelle il est envisagé de traiter des données à caractère personnel. Il ne doit pas, par principe, prêter à équivoque, ce qui exclut de considérer le silence comme une indication d'acceptation ou de refus. En conséquence, un « accord général » de la personne concernée, par exemple en vue de la collecte par vidéosurveillance de données la concernant, n'équivaudrait pas à un consentement aux termes de l'article 2 h) de la Directive.

74. cc) Le consentement doit être informé. Par consentement « informé », il faut entendre le consentement donné par la personne concernée sur la base d'une appréciation et d'une compréhension des faits et des implications d'une action. Il convient de donner à la personne concernée, de manière claire et compréhensible, des informations précises et complètes sur toutes les questions pertinentes, en particulier celles énoncées aux articles 10 et 11 de la Directive, comme la nature des données traitées, les finalités du traitement, les destinataires de transferts éventuels et les droits de la personne concernée. Cela suppose aussi que la personne soit consciente des conséquences du refus de consentir au traitement en question.

75. Dans un nombre croissant de situations, la vidéosurveillance pour des raisons de sécurité est si largement utilisée que les personnes s'attendent même à ce qu'elle soit installée dans des lieux semi-publics ou semi-privés comme des banques, des stades, des aéroports, des gares ou des magasins. Dans certains pays et dans certains cas, il peut même être obligatoire d'installer des vidéos pour des raisons de sécurité. Dans ces situations, l'usager s'attend même d'ailleurs à pénétrer, pour des raisons de sécurité, dans une zone placée sous surveillance vidéo

76. Dans ce contexte et de ce fait, le visiteur peut n'avoir d'autre choix que de « consentir », faute de quoi il risque de se voir refuser l'accès au lieu et au service.

77. Par ailleurs, si l'on part du principe que le consentement est systématiquement donné au motif qu'il faut s'attendre à une surveillance, le droit au respect de la vie privée ne serait exercé que dans un nombre très restreint de lieux privés.

78. De plus, la liberté du propriétaire/gérant des lieux n'est pas illimitée s'agissant de savoir avec précision où et comment la surveillance est exercée et comment les données sont traitées. Par exemple, les visiteurs sont en droit de penser que les zones généralement considérées comme rigoureusement privées ne seront pas placées sous surveillance contrairement à des espaces plus vastes, comme les toilettes et les salles de bains. Dans les

---

[14] Organe consultatif européen indépendant auprès de la Commission européenne sur la protection des données et de la vie privée (« Groupe de travail ″article 29″ » sur la protection des données »).

[15] Voir également l'« avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel » du Groupe de travail ″article 29″ (WP 84, Section 10).

hôtels et les maisons d'hôtes, on s'attend à ce qu'il y ait une surveillance dans les vestibules et les couloirs, mais non dans les chambres. Cela étant, même si il y a lieu de prévoir une surveillance, la personne qui l'exerce n'est pas libre de traiter comme elle le souhaite les données collectées.

***

79. La question du consentement est capitale en cas d'enregistrement d'opérations dans des situations rigoureusement privées ou familiales, par exemple s'agissant de la gestion de ce qu'il est convenu d'appeler les « nounou-cams » ou les caméras à usage familial. Ces caméras permettent aux parents d'observer ce que leurs employés ou domestiques font lorsqu'ils sont chez eux avec leurs enfants. Dans ce cas, le consentement de l'employé devrait être exigé par la loi.

D. Quelle protection la législation nationale peut-elle offrir ?

80. Compte tenu de l'obligation positive décrite ci-dessus, l'Etat doit veiller à ce que la surveillance des lieux privés ou publics par des opérateurs privés puisse se justifier d'après les critères énoncés au deuxième paragraphe de l'article 8 de la CEDH : la surveillance est (a) prévue par la loi ; (b) nécessaire dans une société démocratique ; et (c) 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.

81. L'avis précédent de la Commission de Venise sur la vidéosurveillance dans les lieux publics par les autorités publiques donnait un aperçu général des dispositions nationales applicables à la vidéosurveillance et à la protection des données au niveau constitutionnel[16] ou législatif[17].

82. D'après l'organe consultatif européen indépendant de la Commission européenne sur la protection des données et la vie privée (le « Groupe de travail « Article 29 » sur la protection des données), plusieurs Etats membres ont déjà adopté des réglementations ou des dispositions particulières au sujet de la vidéosurveillance et de sa supervision[18-19]. Dans le cadre de ces réglementations, l'installation et l'utilisation de la TVCF et de dispositifs de surveillance analogues doivent être autorisées à l'avance par l'autorité nationale de protection des données directement ou par un organe administratif qui la représente en tout ou en partie.

---

[16] Voir le paragraphe 34 du document CDL-AD(2007)014 « Le droit à la vie privée est expressément protégé au niveau constitutionnel dans la quasi-totalité des Etats membres du Conseil de l'Europe (CdE) ». Voir par exemple dans CODICES la Constitution des pays suivants : Andorre (articles 13 et 14), Arménie (articles 20 et 21), Autriche (article 10), Azerbaïdjan (article 32), Belgique (article 22), Bosnie-Herzégovine (article 3), Bulgarie (article 32), Chypre (article 15), Croatie (article 35), Espagne (article 18), « ex-République yougoslave de Macédoine » (article 25), Fédération de Russie (article 23), Finlande (section 10), Géorgie (article 20), Grèce (article 9), Hongrie (article 59), Irlande (articles .40-42-44-45), Islande (article 71), Lettonie (article 96), Lituanie (article 22), Malte (article 32), Moldova (article 28), Pays-Bas (article 10), Pologne (articles 30 et 31), Portugal (article 26), République de Slovénie (article 35), République slovaque (articles 19 à 21), Roumanie (article 26), Suède (chapitre 1, article 2), Suisse (article 13), Turquie (article 20), Ukraine (article 32).

[17] Voir le paragraphe 38 du document CDL-AD(2007)014. Pour une vue d'ensemble de la législation nationale relative à la protection des données et de ses principales dispositions, voir le tableau à l'adresse suivante : http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/National_laws/index.asp#TopOfPage

[18] Allemagne, Danemark, Espagne, Finlande, France, Grèce, Irlande, Italie, Luxembourg, Pays-Bas, Portugal, Suède.

[19] Pour un complément d'information, voir le document WP89, n° 4/2004, adopté le 11 février 2004, note de bas de page 5 (www.europa.eu.int/privacy).

83. Les réglementations peuvent être différentes selon que l'entité chargée de l'activité de vidéosurveillance relève du secteur public ou du secteur privé.

84. La législation nationale relative à la protection des données à caractère personnel prévoit aussi d'ordinaire des obligations et des interdictions pour les particuliers.

85. Ainsi, aux Pays-Bas, la loi sur l'enregistrement des personnes définit aussi les conditions et les restrictions applicables à l'enregistrement dans des locaux privés. Cette loi exige notamment que l'enregistrement se fasse dans un but raisonnable, soit conforme à la loi, ne soit pas contraire à l'ordre public et à la morale, ne soit pas utilisé à une fin autre que celle pour laquelle il est effectué et fasse l'objet d'une protection adéquate contre la perte, le vol et l'utilisation non autorisée. Elle prévoit aussi que les données collectées ne peuvent être communiquées à des tiers que si cette communication résulte de l'objet de l'enregistrement, est exigée par la loi ou se fait avec l'autorisation de la personne concernée.

86. Certains pays, comme la Belgique et la France, ont prévu des dispositions particulières de droit pénal concernant un « droit à l'image ». Toute personne a un droit exclusif sur son image et pourrait en empêcher la diffusion. En France, l'article 226-1 du Code pénal interdit de capter, d'enregistrer ou de transmettre l'image d'une personne ou un photomontage d'elle sans son consentement.

87. La licéité, en droit interne, du procédé de vidéosurveillance doit être traitée non seulement en fonction des critères énoncés à l'article 8.2 de la CEDH, incorporés dans le droit interne, mais aussi en fonction de critères supplémentaires comme ceux énoncés dans la « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » et la Directive 95/46/CE.

E. Garanties supplémentaires

a. concernant le droit d'être informé

88. Le public doit être informé comme il convient de la présence de caméras[20]. Comme dans le cas de la vidéosurveillance des lieux publics par les autorités publiques, la personne qui a des raisons de penser que des données la concernant ont été enregistrées dans un lieu privé par un particulier ou une autorité publique a le droit d'exiger d'avoir accès à ces données, de les corriger ou de les détruire et également d'être informée de tout usage qui en est fait par la personne qui les a collectées ou par une autre personne auxquelles elles ont été transférées.

b. concernant le traitement

89. Les données à caractère personnel faisant l'objet d'un traitement entièrement automatisé doivent être obtenues et traitées loyalement et licitement ; être enregistrées pour des finalités déterminées et légitimes et ne pas être utilisées de manière incompatible avec ces finalités ; être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ; être exactes et, si nécessaire, être mises à jour ; être conservées sous une

[20] En France par exemple, la CNIL (Autorité française de protection des données) donne l'exemple d'un panneau d'information qui devrait être visible à l'entrée d'un établissement sous vidéosurveillance : le texte ci-après doit figurer à côté du graphique d'une caméra.

> *« nous vous informons que cet établissement est placé sous vidéosurveillance pour des raisons de… [indiquer les finalités poursuivies], pour tout renseignement, s'adresser au service … ou à … [identifier la personne ou le service compétent] auprès duquel vous pouvez également exercer votre droit d'accès, conformément à la loi 78-16 du 6 janvier 1978 relative à informatique, aux fichiers et aux libertés modifiée par la loi du 6 août 2004 ».*

forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaires aux finalités pour lesquelles elles sont enregistrées.

90. En d'autres termes, aucune donnée ne devrait être conservée sauf nécessité absolue et dans ce cas uniquement pendant une durée déterminée.

c. concernant l'accès

91. Les personnes peuvent avoir accès aux données collectées qui les concernent[21]. Elles sont aussi en droit d'être informées de la collecte et du traitement de ces données, que ces dernières aient été transmises à d'autres personnes ou institutions, et de l'utilisation qui en sera faite.

92. Les points traités jusqu'à présent laissent certaines questions en suspens qui ne relèvent normalement pas du débat relatif à la surveillance. L'une d'entre elles est « l'effet dissuasif » créé par l'impression d'être constamment surveillé par « Big Brother », ce qui inhibe la liberté de chacun en matière de comportement, de mouvement et d'expression[22]. Ce sentiment peu plaisant et frustrant d'être observé et entravé peut exister même si les caméras sont factices et si il n'y a pas de caméras derrière le panneau.

93. Cette situation renforce la crainte de voir les sociétés modernes s'orienter vers un contrôle total et devenir de plus en plus impersonnelles comme envisagé dans les romans de contre-utopie « Nous autres » de Zamiatine, « 1984 » et d'Orwell et dans les indications données par Foucault dans « Surveiller et punir » (le principe du panoptique).

94. Ces préoccupations, actualisées par l'augmentation spectaculaire des possibilités technologiques de contrôle total, montrent que la réglementation juridique devrait être tout à fait novatrice et ne pas se limiter à des amendements à la législation en vigueur.

IV. Conclusions et recommandations

95. L'extention récente de la vidéosurveillance est commune à tous les pays contemporains développés, qu'il s'agisse de caméras exploitées de manière privée ou publique.

96. Comme la vidéosurveillance par des opérateurs privés ne saurait être raisonnablement évitée ou interdite, une analyse critique et une action concertée s'imposent de toute urgence pour fixer certaines limites aux activités des opérateurs publics ou privés.

97. La Commission de Venise estime que de nouvelles réglementations inventives, que ce soit aux niveaux national, européen et international, s'imposent pour faire face à la menace qui pèse sur les droits fondamentaux comme les droits à la vie privée et à la liberté de circulation ainsi que le droit de bénéficier d'une protection particulière en ce qui concerne les données à caractère personnel qui sont collectées.

98. Des règles juridiques devraient s'appliquer à toutes les situations dans lesquelles une surveillance est exercée, dans l'espace public, privé et semi-privé, ainsi qu'à tous les opérateurs, publics et privés, y compris aux opérateurs privés auxquels des fonctions publiques sont déléguées.

---

21 Voir la note de bas de page 20.

22 Cette question a été soulevée en 1996 par Pierre Herbeq au nom de la Ligue belge des droits de l'homme devant la Commission européenne des Droits de l'Homme. La requête de M. Herbeg a été déclarée irrecevable (*Herbeq c. Belgique,* 14 janvier 1998, requête n° 32200/96, 92 D.R. 92).

99. La Commission de Venise réitère en conséquence les recommandations qu'elle a formulées dans son étude précédente :

- 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 les conditions posées par la Directive 95/46/CE, notamment à ses articles 6[23] et 7[24] qui reprennent l'article 5 de la Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[25].

100. Par ailleurs, compte tenu des particularités de la vidéosurveillance, la Commission recommande de prendre systématiquement les mesures suivantes :

- Le public doit être prévenu qu'il est surveillé 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.

---

23 Aux termes de l'article 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 ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et 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…

24 L'article 7 prévoit que le traitement de données à caractère personnel ne peut être effectué que si :

- « la personne concernée a indubitablement donné son consentement ;
- il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
- il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique … ;
- il est nécessaire à la réalisation de l'intérêt légitime poursuivi…, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée… »

25 L'article 5 de la Convention est libellé comme suit :

« 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 ».

- Une autorité indépendante spécialisée doit être mise en place, comme plusieurs pays européens l'ont fait[26], 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.

101. Une personne qui a des raisons de penser qu'elle a fait l'objet d'une surveillance et que des données la concernant ont été enregistrées devrait avoir le droit de demander à avoir accès aux données et à les corriger ou à les détruire sauf si des raisons de sécurité doivent primer pendant un certain délai. Elle devrait aussi avoir le droit d'être informée de toute utilisation qui est faite de ces données par la personne qui les a réunies ou par toute autre personne à laquelle les données ont été transférées.

102. L'ensemble du dispositif de surveillance devrait être approuvé et sous licence et être accessible pour que les autorités effectuent des contrôles périodiques si les circonstances l'exigent.

[26] Obligation énoncée à l'article 28 de la Directive 95/46/CE pour tous les Etats membres de l'UE et de l'Espace économique européen.