Télésurveillance

- Gazette - Débats -

Date de mise en ligne : dimanche 14 dcembre 2008

Revue du Mauss permanente

Il est maintenant acquis que la vidéosurveillance n a qu un effet marginal sur la criminalité voire un effet négatif, si on la compare, en termes d investissement financier, à d autres mesures telles que l amélioration de l éclairage public ou le recrutement et l équipement des forces de police [1]. Le 6 mai dernier, le responsable du bureau des images, identifications et détections visuelles (*Viido*) de la police métropolitaine de Londres (*Scotland Yard*) qualifiait d ailleurs publiquement la vidéosurveillance au Royaume-Uni leader mondial en la matière avec plus de 4,2 millions de caméras de "véritable fiasco" [2].

Cette incapacité complète à remplir la fonction qu on leur assigne fait des caméras de bien étranges objets. Ne sont-elles que des boîtes noires inertes, aveugles ? La croissance à deux chiffres du marché de la vidéosurveillance depuis quinze ans suggère pourtant que cette technologie encore relativement nouvelle suscite l enthousiasme [3]. C est même principalement et paradoxalement la croyance fanatique en la toute-puissance des caméras qui explique que celles-ci soient aussi inefficaces.

C est en effet parce que l on conçoit les caméras comme un "remède miracle" [4] à la délinquance que l on procède massivement à leur installation en s abstenant de s interroger sur les mécanismes précis grâce auxquels ce miracle doit opérer. Au lieu de réfléchir à la manière dont les caméras vont prévenir des délits aussi divers que le cambriolage, le trafic de stupéfiants ou le vandalisme, on leur suppose un pouvoir parfaitement décontextualisé, ou trans-contextuel, *magique* : celui de "réduire la criminalité". Le résultat est que, plutôt que d avoir un effet homogène sur l ensemble des actes criminels, la vidéosurveillance n est utile contre aucun désordre en particulier.

C est ensuite parce que l on suppose aux caméras un fonctionnement non seulement automatique, mais autonome, que l on privilégie la sophistication technologique à la formation des opérateurs chargés de visionner les écrans, et au travail de coordination avec les services de police. Pourtant, comme le rappelle Gavin Smith, de l université d Aberdeen : « les caméras de surveillance ne sont ni conscientes, ni autonomes, et pour être efficaces elles exigent d être constamment sous le regard et le contrôle d êtres humains opérants dans un contexte de travail qui puissent visionner, interpréter et réagir aux millions d images produites ». [5]

Or, l aspect humain des réseaux de vidéosurveillance est tellement négligé que la difficulté des opérateurs à reconnaître "un comportement suspect" [6] pourtant le seul comportement qui soit censé mériter leur attention provoque des tensions avec les services de police, avec lesquels les relations sont gérées au cas par cas, et sont souvent rares [7]. Par ailleurs, il n est pas exceptionnel que chaque opérateur soit chargé de surveiller individuellement une quinzaine de caméras. Le rôle minimal que tient la médiation humaine dans l exercice de la vidéosurveillance témoigne ainsi d une "forme naïve de déterminisme technologique" [8] ; autrement dit, il semble l on attende des caméras qu elles s utilisent toutes seules.

C est enfin parce que l efficacité des caméras tient de l évidence première dans l imaginaire collectif que les études qui remettent en cause l infaillibilité des caméras suscitent l incrédulité, tandis que les clichés extraordinaires des grandes affaires médiatiques passent pour représentatifs du cours normal de la vidéosurveillance. *This Is London* par exemple s étonne encore en 2005 des résultats d *Assessing the Impact of CCTV* , "rapport surprise du gouvernment" selon lequel "la vidéosurveillance est d une très faible utilité dans la lutte contre la criminalité" [9]. Or, un système que l on imagine au-delà de tout dysfonctionnement est un système soustrait à la critique, donc qui ne se réforme pas.

Les caméras de surveillance sont ainsi des objets auxquels on se rapporte comme s ils disposaient d une puissance automatique, autonome et infaillible, quel que soit leur pouvoir réel, et *quels que soient les effets de cette croyance sur la réalité de ce pouvoir*. On peut y voir l aveu indirect que les caméras accomplissent une autre fonction que celle

de lutter contre la délinquance. Comme le soulignent d ailleurs dans leur conclusion les auteurs d *Assessing the Impact of CCTV*, "le taux de criminalité n est pas un bon indicateur de l efficacité de la vidéosurveillance".

Une idée que semblent partager les habitants du complexe de tours de Hutchesontown, à Glasgow. Interrogés en 1996 à propos d un système de vidéosurveillance installé deux ans auparavant à l intérieur et aux alentours de leur ensemble d immeubles, plus de 90% des résidents déclaraient trouver que le réseau était "bénéfique pour la communauté", alors que seulement 50% des résidents déclaraient avoir constaté une "une diminution du taux de criminalité" depuis l installation des caméras. Les statistiques policières n indiquent quant à elle aucune variation significative du taux de criminalité [10]. « Même quand [le public] conclut que la vidéosurveillance ne réduit pas la criminalité", notent ainsi Martin Gill et Angela Spriggs (*Assessing the Impact of CCTV*), "il continue d être majoritairement en faveur de son utilisation. »

Par quel biais comprendre alors le phénomène de la vidéosurveillance ? Le regard des caméras repose d abord sur une division de l espace social entre espace "public" et espace "privé". C est en effet à la limite de l espace "privé" que le regard des caméras est jugé devoir s arrêter ; c est au-delà de cette limite qu on le juge intrusif et illégitime. Mais qu entend-on par espace privé ? Où commence, où s arrête le domaine de ce qui est confidentiel ? La plupart des rapports officiels et des études universitaires s accordent à trouver la notion de "confidentialité" (*privacy*) problématique. Simon Davies, directeur de *Privacy International*, n hésite pas à qualifier le droit à la confidentialité de "droit le plus nébuleux (*unruly*) de tous les droits de l humain", tandis que Raymond Wacks, auteur de nombreux ouvrages sur le sujet, juge le terme de "confidentialité" vide de sens tellement il est investi de significations variées, voire contradictoires [11].

Il en existe pourtant une définition à la fois précise et tout à fait opératoire, que formule entre autres Alan Westin, professeur de droit et d administration publics à l université de Columbia :

« La confidentialité (*privacy*) est la possibilité pour des invidus, des groupes, ou des institutions de déterminer eux-mêmes quand, comment et avec quel degré de précision des informations qui les concernent sont communiquées à autrui. » [12]

L idée d un *consentement* sert notamment à définir la confidentialité en médecine, où, comme le rappelle un rapport de l *Information Commissioner s Office* britannique, les données jugées "confidentielles" : « ne doivent être utilisées qu à la seule fin pour laquelle elles ont été recueillies. Toute nouvelle utilisation requiert donc un nouveau consentement signé de la part de chaque patient concerné ». [13]

C est aussi la définition employée pour définir le droit à l image, à la reproduction d oeuvres ou d articles, etc. La référence au consentement est une façon de reconnaître que l individu doit pouvoir exercer un contrôle sur ce qui lui est "confidentiel", précisément parce que c est confidentiel.

S agissant de vidéosurveillance cependant, ce critère s avère impossible à retenir.

Empiriquement, d abord, il est improbable de prétendre obtenir un véritable consentement de la part des individus filmés. Le droit européen oblige au signalement manifeste des réseaux de caméras, mais il est difficile de soutenir que les individus acceptent effectivement de renoncer à toute confidentialité dès lors qu ils s aventurent dans une zone surveillée, simplement parce qu ils en sont avertis. Ce pseudo-consentement est du reste jugé si peu significatif que plus de 50% des réseaux dans les capitales européennes ne sont pas signalés du tout [14].

Mais surtout, une définition de la confidentialité par le consentement est structurellement exclue par les technologies

de surveillance :

Il est impossible de prédire les résultats d une analyse de données menée à l aide d une technologie conçue pour découvrir des relations non-évidentes. Cela veut dire que les compagnies sont incapables de pleinement informer leurs clients quant à l utilisation qui va être faite des données qui les concernent, car les catégories produites par l analyse des données sont émergentes. De plus, le principe d une limitation de l utilisation de l information va à l encontre du fonctionnement même du système. Plus la base de données est grande et les combinaisons potentielles sont nombreuses, plus les prédictions qu opère le système sont précises. [15]

En matière de vidéosurveillance, donc, comme de surveillance en général, "l utilisation des données ne peut être clairement spécifiée" [16]. Une fois enregistrées, il est impossible de prédire comment les données seront lues ou interprétées. Les termes d un consentement éventuel seraient ainsi nécessairement trop vagues pour être recevables.

De ce fait, plutôt que de préciser quel niveau d information suffit à rendre un consentement valable, ou quel mode d expression le consentement doit prendre en quelles circonstances, les textes officiels tentent de définir la confidentialité en délimitant des régions de la réalité plus ou moins "confidentielles".

Ainsi, la Commission Européenne pour la Démocratie par le Droit écrit que : « La vie privée est une sphère très large qui n est pas facile à définir ; elle ne se limite pas à un "cercle intime" dans lequel l individu vit sa vie personnelle ». [17]

Le droit allemand reconnaît quant à lui trois "sphères" de confidentialité : la sphère intime (*Intimsphäre*), la plus protégée ; la sphère élémentaire (*die schlichte Privatsphere*) ; enfin, la sphère individuelle (*Individualsphäre*) [18].

Le problème devient donc celui de déterminer quel degré de confidentialité est objectivement attribuable aux choses ou aux espaces, indépendamment de tout consentement subjectif [19]. C est la règle de la *proportionnalité* des informations collectées ou transmises qui permet de décider objectivement du juste degré de confidentialité à respecter en chaque circonstance, c est-à-dire que, selon la *Royal Academy of Engineering* "la collection de données et la surveillance sont fondamentalement légitimes quand elles sont effectuées dans l intérêt du citoyen" [20]. Il s agit donc d équilibrer la perte de "confidentialité" avec les "bénéfices" de la surveillance, sans que soit clair à qui il revient d effectuer ce calcul, puisque les individus n ont plus un contrôle privilégié sur les données qui les concernent.

Dès lors, "la notion de confidentialité est intrinsèquement contingente et polémique, soumise aux transformations de la société et de la technologie", et "doit être constamment redéfinie." [21] Autant dire qu elle est vidée de tout contenu.

Pour éviter l écueil d un relativisme pur et simple cependant, la plupart des institutions retiennent une définition minimale de la confidentialité comme ce qui relève du personnel, c est-à-dire comme *ce qui permet l identification de chaque individu en propre*. "Les données personnelles", explique par exemple l *Information Commissioner s Office*, "sont celles qui concernent une personne vivante qui peut être identifiée grâce à ces données, seules ou en conjonction avec d autres données." [22]

C est cette définition de la confidentialité qu exprime la métaphore domestique, couramment invoquée pour délimiter ce qui relève du confidentiel en matière de vidéosurveillance. Avouant ne pas avoir lu le guide d utilisation du réseau dont il a la charge, ni même savoir où celui-ci se trouve, un des opérateurs interrogés par Gill et Spriggs se justifie

ainsi de façon caractéristique : « &on n a jamais vraiment eu besoin de le consulter de toute façon& la plupart de ce qu il y a là-dedans, c est des choses qu on sait déjà, comme de ne pas regarder chez quelqu un par la fenêtre& » [23]

La municipalité de Loughborough, quant à elle, n impose typiquement comme seule limite inconditionnelle au regard de ses 24 caméras "la surveillance de l intérieur de domiciles, d entreprises ou d autres locaux privés." Une "cause raisonnable" suffit pour lever la confidentialité de tout le reste de l univers social, c est-à-dire pour en légitimer la vidéosurveillance [24].

Prise à la lettre, cette conception de la confidentialité revient en effet à considérer comme parfaitement public tout ce qui n est pas personnel, c est-à-dire tout ce qui n est pas *associable à un nom propre*. C est ainsi que la municipalité de Brentwood a pu fournir à une chaîne de télévision nationale britannique les images d une tentative de suicide en pleine rue (sans autre témoin que les caméras). La municipalité avait jugé que, du moment que le visage de l individu était masqué, cet acte n avait plus rien de confidentiel puisque la tentative s était produite dans un lieu public. "Cause" suffisamment "raisonnable" selon la municipalité pour livrer ces images (pourtant extrêmement intimes) à la diffusion, la volonté d informer ses citoyens de l utilité du système de vidéosurveillance municipal fraîchement installé : l intervention de la police, alertée par un opérateur, avait permis d empêcher le suicide [25].

Le regard des caméras supposerait ainsi de partager l espace social entre des espaces privés, chacun associé à un nom propre, et un espace public défini alors par *la rencontre d au moins deux noms propres*. Tout espace interpersonnel se verrait donc assigner une transparence de droit. L espace public ainsi conçu serait celui d une surveillance normale de tous par tous. La scrutation des caméras tiendrait sa justification du fait qu elle ne ferait que reprendre pour l intensifier le regard que chacun porterait légitimement sur chacun. Symptomatique de cette conception, une déclaration que des chercheurs scandinaves qualifient de courante : "De toute façon, je ne fais rien de secret. Que des gens m observent directement ou via des caméras ne fait pour moi aucune différence" [26].

En réalité cependant, la séparation qu introduit la vidéosurveillance entre espace public et espace privé repose plutôt sur une logique normative que sur une opposition entre personnel et impersonnel. Certaines normes instruisent la surveillance pour soustraire à l oeil des caméras certaines conduites, donc certaines catégories d individus. A l instar de la ville de Leicester, de nombreuses municipalités précisent par exemple dans leur code d utilisation qu il "ne sera pas fait usage du réseau de vidéosurveillance pour poursuivre les auteurs de violations mineures du code de la route" [27]. "De cette manière", commentent les chercheurs Clive Norris et Gary Armstrong, "la sous-représentation des contrevenants plus vieux et plus aisés est gravée dans les procédures opératoires du système, qui atténuent l impact sur ceux-ci du scrutement par les caméras". [28]

La vidéosurveillance autorise donc un champ particulier de comportements et d identités, et en interdit d autres. Elle n ouvre pas tant les espaces privés au regard public qu elle ne soumet l espace public à des normes privées, c est-à-dire, le privatise. Les 66% d Européens qui affirment qu ils n ont "rien à craindre" des caméras car ils n ont "rien à cacher", comme les 25% qui déclarent qu ils "se sentiraient plus en sécurité avec des caméras partout" [29], expriment ainsi, non pas la complète publicité de leurs personnes comme s ils n avaient effectivement "rien à cacher" mais plutôt la certitude intime que le regard des caméras ne se portera pas sur eux, comme s ils évoluaient dans un espace privé. La vidéosurveillance construit l espace public selon un cadre normatif qu ils reconnaissent comme le leur. En somme, ils déclarent se sentir dans l espace sous surveillance comme chez eux. [30]

Les personnes qui se départissent de certaines normes sollicitent en revanche l attention assidue des caméras, car elles sont *chez autrui*. « Le regard des caméras ne se porte pas de façon égale sur tous les utilisateurs de l espace urbain" remarquent ainsi Norris et Armstrong, qui notent que 93% des individus surveillés sont de sexe masculin, que 86% ont moins de 30 ans, ou encore, que 68% des noirs soumis à une attention particulière le sont "sans raison apparente. » [31]

Dans une certaine mesure, on peut dire que ce visionnage discriminatoire résulte du fonctionnement de la technologie elle-même. Comme le soulignent les berlinois Leon Hempel et Eric Töpfer, le fait de devoir trier rapidement un très grand nombre d images pousse les opérateurs à se focaliser "sur une gamme étroite de caractéristiques facilement repérables plutôt que sur des comportements suspects". "La limitation sensorielle des écrans", ajoutent-ils, encourage cette attitude en augmentant "la distance entre celui qui observe et celui qui est observé" [32]. La vidéosurveillance opère donc en identifiant des catégories d individus plutôt que des actes individuels. Le passage à la technologie numérique facilite plus encore le vidéo-stéréotypage, avec des procédés tels que la reconnaissance faciale.

Le choix des catégories que les caméras repèrent dépend cependant des intérêts du groupe social qu elle servent. Emmanuel Martinais et Christophe Bétin, chercheurs au CNRS, soulignent par exemple que la cinquantaine de caméras que compte la presqu île de Lyon depuis 2001 sont l instrument explicite d une lutte des "commerçants et de certains résidents" contre une population "assez jeune", "d origine Nord-Africaine" et désignée comme "issue des quartiers dits sensibles" [33]. Le "délinquant typique" que les caméras poursuivent de leur regard ressemble en tous points au "jeune des banlieues", dont la présence est jugée nuire à l attractivité des commerces. Les responsables du réseau de vidéosurveillance expliquent ainsi que : « le système est loin d être capable de réduire toutes les formes de criminalité, mais il se montre particulièrement utile et efficace pour lutter contre le phénomène bien connu de la délinquance importée. »

L extériorité normative est spontanément interprétée comme une extériorité spatiale : la "délinquance" est "importée", car les "jeunes" sont forcément "des banlieues". Or, en 1999, seuls 25% des délits enregistrés dans la presqu île étaient attribuables à des personnes venues de banlieue lyonnaise. "Les comportements ne sont pas qualifiés de criminels en fonction de normes légales", commentent Martinais et Bénin, mais en fonction du "désir de quelques-uns de renforcer leur domination sur un espace qui est censé appartenir à tout le monde." Cette appropriation de l espace suppose que certains soient considérés comme des intrus, à évincer, ou au moins à soumettre à un contrôle sévère.

La vidéosurveillance ne menace donc pas tant les espaces privés que l espace public. Si "pour pouvoir contribuer à l intégration sociale, les espaces partagés doivent être perçus comme attrayants, sûrs, accueillants et inviter à l exercice d une vaste gamme d activités" [34], alors les caméras sont des outils de désintégration sociale. Elles délimitent un territoire caractérisé par une fermeture de l espace public via sa soumission à des normes et intérêts privés. Les capacités fantastiques que l on prête aux caméras témoignent d ailleurs du plaisir narcissique qui accompagne cet acte d appropriation, c est-à-dire, des pulsions régressives qui animent le développement de la vidéosurveillance.

Noé le Blanc

---

[1] Cf. mon article L oeil Myope des caméras, Le Monde Diplomatique, Septembre 2008. Pour l année 1995, par exemple, deux chercheurs du Scottish Centre for Criminology ont établi que les 32 caméras du centre-ville de Glasgow n avaient contribué qu à une seule arrestation par caméra toutes les 967 heures de surveillance, soit à une arrestation tous les 40 jours (Ditton, Jason & Short, Emma, Yes it works, no, it doesn t : comparing the effects of open-street CCTV in two adjacent town centres, Scottish Centre for Criminology, 1999). En 1999, les britanniques Clive Norris et Gary Armstrong ont dénombré quant à eux à peine 12 arrestations liées aux caméras sur 592 heures de surveillance dans trois centre-villes (Norris, C. and G. Armstrong The Unforgiving Eye : CCTV Surveillance in Public Space, University of Hull, 1997). Les progrès techniques réalisés depuis les années quatre-vingt-dix n ont permis aucune amélioration de ce bilan. Des chiffres de la police londonienne obtenus grâce au Freedom of Information Act en septembre 2007 révèlent notamment l absence de corrélation entre le taux d élucidation des délits et le nombre de caméras installées. En effet, tandis que le borough de Brent, qui ne dispose que de 164 caméras sur voie publique, possède le meilleur taux d élucidation du Grand Londres (25,9%), le borough de Wandsworth, qui en compte 993, n atteint pas la moyenne londonienne de 21% de délits élucidés ; non plus que les boroughs de Tower Hamlets (824 caméras), de Greenwich (747), ni de Lewisham (730)

(This Is London, 19/09/07).

[2] "an utter fiasco", selon le Deputy Chief Inspector Mike Neville. Viido est l abréviation de Visual Images, Identifications and Detections Office. Selon les déclarations de ce responsable, la vidéosurveillance n a permis d élucider que 3% des vols en pleine rue à Londres, par exemple, malgré les 500 000 caméras que compte la capitale britannique, soit une pour 14 habitants.

[3] Cf. encore L oeil Myope des Caméras, in Le Monde Diplomatique, Septembre 2008.

[4] Voir par exemple les déclarations de J. Ditton le 14/07/1999 à la BBC, selon lequel la vidéosurveillance a été "vastement surévaluée" et a été présentée "au moment de son introduction" en Grande-Bretagne comme une "solution miracle à tout". http://news.bbc.co.uk/1/hi/uk/394021.stm

[5] Smith, Gavin, Behind the Screens : Examining Constructions of Deviance and informal Practices among CCTV Control Room Operators in the UK, Surveillance & Society CCTV Special , 2004.

[6] "La partie la plus déficiente de la formation concerne comment identifier les comportements suspects, quand il est pertinent de suivre des individus ou des groupes, et à quel moment filmer des personnes ou des incidents de plus près. Il est tenu pour acquis que les réponses à ces questions sont évidentes, ou relèvent du bon sens." Bulos, Marjorie et Sarno, Christopher, Codes of Practice and Public Closed Circuit Television Systems, London Local Government Information Unit, 1996.

[7] Cf. Gill, Martin & Spriggs, Angela, Assessing the impact of CCTV, Home Office Research Study 292, 2005.

[8] Norris, Clive & Armstrong, Gary, The Maximum Surveillance Society : The Rise of CCTV as Social Control, Oxford, Berg, 1999.

[9] Édition du 24/02/05.

[10] Evaluation of CCTV Security System at Hutchesontown Multi-storey Blocks, Scottish Homes Précis n 87, 1999.

[11] Gallagher, Caoilfhionn, CCTV and Human Rights : the Fish and the Bicycle ? An Examination of Peck V. United Kingdom, Surveillance & Society CCTV Special , 2004.

[12] Westin, Alan, Privacy and Freedom, New York, Atheneum Press, 1967, cité par Coney, Lillie, Associate Director Electronic Privacy Information Center, in Expectations of Privacy in Public Spaces, Full Committee Meeting of the Department of Homeland Security Data Privacy and Integrity Advisory Committee, Arlington, 07/06/2006.

[13] A Report on the Surveillance Society for the Information Commissioner, Surveillance Studies Network, 2006. L Information Commissioner s Office est l équivalent de la CNIL française.

[14] Hempel, Leon et Töpfer, Eric, Urbaneye final report, Centre for Technology and Society, Technical University Berlin, 2004.

[15] A Report on the Surveillance Society, p.41.

[16] Ibid.

[17] Commission de Venise, Étude n404, Strasbourg, 23/03/2007.

[18] Gras, Marianne, The Legal Regulation of CCTV in Europe, Surveillance & Society CCTV Special, 2004.

[19] Typiquement, le Data Protection Act de 1998, pierre angulaire de la garantie de la confidentialité du traitement des données au Royaume-Uni, prévoit que les données "personnelles" puissent être manipulées et diffusées avec le seul consentement de l institution qui les détient, pourvu que celle-ci y trouve un "intérêt légitime" : preuve que le droit anglais ne considère pas la transmission de données personnelles sans le consentement de l individu concerné comme une rupture du caractère confidentiel de ces données.

[20] The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State, House of Lords Select Committee on the Constitution, Royal Academy of Engineering , 2007. La Royal Academy of Engineering est un think-tank britannique dont les "priorités stratégiques sont de faire progresser le Génie britannique ; de célébrer l excellence et d inspirer la prochaine génération ; et d être à la pointe des débats actuels en guidant la réflexion éclairée et en pesant sur les politiques publiques."

[21] Dilemmas of Privacy and Surveillance, Challenges of Technological Change, Royal Academy of Engineering, 2007.

[22] What price privacy ? The unlawful trade in confidential personal information, presented by the Information Commissioner to Parliament pursuant to Section 52(2) of the Data Protection Act 1998, 2006. Selon ce rapport, qui fait ainsi preuve d une certaine cohérence, le détournement d informations personnelles concernant des célébrités par des papparrazzi ou par des détectives privés constitue l un des risques majeurs que la société de surveillance fait peser sur la confidentialité.

[23] Op. cité, p.85. C est aussi à l espace domestique que renvoie la Convention Européenne des Droits de l Homme, qui définit la confidentialité comme le "respect de la vie privée et familiale, du domicile et de la correspondance." (Article 8)

[24] Loubourough CCTV Town Centre Annual Report, 2004.

[25] Gallagher, Caoilfhionn, op. cité.

[26] Sætnan, Ann Rudinow, Mork Lomell, Heidi et Wiecek, Carsten, Controlling CCTV in Public Spaces : Is Privacy the (Only) Issue ? Reflections on Norwegian and Danish observations, Surveillance & Society CCTV Special, 2004. C est aussi sur la supposition d une transparence légitime au regard public de l espace interpersonnel que reposent la campagne "Attentifs, Ensemble" de la R.A.T.P. (destinée à prévenir les actes de terrorisme), et sa jumelle britannique "Trust Your Senses".

[27] CCTV/Concierge Control Centre Code of Practice, Public Closed Circuit Television System Owned in Whole or in Partnership by the Council Housing Department, 11/2002.

[28] Norris, Clive & Armstrong, Gary - The Maximum Surveillance Society : The Rise of CCTV as Social Control, 1999.

[29] Hempel, Leon et Töpfer, Eric, op. cité

[30] L aveu indirect, de la part de la Royal Academy of Engineering, de la nécessité d une surveillance discriminatoire, est à ce titre révélateur :« Les bénéfices qu apporte une surveillance totale sont insuffisants au vu du fait qu elle implique l observation de citoyens innocents, qui doivent ainsi subir une diminution de leur confidentialité.(&) Collecter et détenir des informations sur les déplacements et les occupations quotidiennes des personnes, quand ces occupations sont parfaitement légales, devrait être considéré comme une atteinte au droit à la confidentialité. » Autrement dit, la surveillance des individus "innocents" est illégitime en elle-même, car elle place ces individus dans une situation d extériorité par rapport à un espace qui leur revient. Ces remarques n amènent pas à contester en bloc tout projet de surveillance, au nom de la présomption d innocence ; elles suggèrent plutôt que le sens d une surveillance légitime est de ne surveiller que les "coupables".

[31] "for no obvious reason", Norris, Clive & Armstrong, Gary, CCTV and the Social Structuring of Surveillance, Crime Prevention Studies, volume 10, 1999.

[32] Op. cité.

[33] Martinais, Emmanuel et Bétin, Christophe, Social Aspects of CCTV in France : the Case of the City Centre of Lyons, Surveillance & Society CCTV Special , 2004.

[34] Sætnan, Ann Rudinow, Mork Lomell, Heidi et Wiecek, Carsten, op. cité. Les auteurs ajoutent : "Nous comprenons aussi la question du droit à l accès à l espace public comme une extension du droit à la confidentialité : le droit à l accès à l espace public sans discrimination liée à l apparence personnelle ni à des actes qui relèvent du domaine du privé/du choix personnel/de l égalité des droits, tels que le port de certains vêtements, l expression d opinions, les choix de son orientation sexuelle, etc."