La protection des données en relation avec la surveillance (2000) et Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données à caractère personnel au moyen de la vidéo-surveillance), préparé par M. Giovanni Buttarelli

Secrétaire Général de l'Autorité italienne de protection des données (Italie)

Rapport sur la protection des données en relation avec la surveillance

Avertissement

L'importance du phénomène et des activités de surveillance au moyen de techniques toujours plus performantes requière une réflexion approfondie tant au niveau national qu'au niveau international en ce qui concerne les avantages et risques pour nos sociétés démocratiques et les individus.

Plusieurs Etats ont entamé des travaux dans ce domaine tout en considérant qu'il conviendrait d'élaborer des dispositions législatives spécifiques de protection des données dans le domaine de la (vidéo-)surveillance.

Dans ce contexte, le Conseil de l'Europe a souhaité appeler l'attention sur certains aspects particuliers de la surveillance. Le Groupe de Projet pour la Protection des Données (CJ-PD) du Conseil de l'Europe a sollicité d'un consultant, le Dr Giovanni BUTTARELLI, un rapport sur la protection des données en relation avec les activités de surveillance. Ce rapport reconnaît que toute étude sur la surveillance est liée à l'évolution technologique des moyens de contrôle et doit donc être située dans son contexte historique.

On a donc souhaité mettre en évidence une liste de principes directeurs spécifiques à la vidéo-surveillance qui mériteraient d'être pris en considération lors de l'élaboration de dispositions législatives spécifiques en relation avec la vidéo-surveillance. Ces principes pourraient le cas échéant être appliqués à d'autres formes ou techniques de surveillance avec les aménagements nécessaires.

Le rapport de M. Buttarelli et les principes directeurs ont été diffusés sur le site Web du Conseil de l'Europe en décembre 2000, sollicitant les réactions du public. Les seuls commentaires reçus émanèrent de la Table Ronde internationale sur les communications, qui pense que ces principes ne doivent s'appliquer qu'à la vidé-surveillance, et non à tous les autres secteurs de la surveillance. Sur la base du rapport et des principes directeurs, préparés par M. Buttarelli, le CJ-PD a décidé d'élaborer un projet des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéo-surveillance. Les membres du CJ-PD ont été priés d'envoyer des commentaires écrits, finaux, sur les projets de principes directeurs du Groupe de co-ordination du CJ-PD (juin 2002). Le Groupe de co-ordination soumettra les projets de principes directeurs au CJ-PD pour examen et adoption lors de sa réunion d'octobre 2002.

1) INTRODUCTION

Chaque étude ou rapport sur la surveillance est lié à l'évolution technologique des systèmes de contrôle et doit donc être situé dans son contexte historique.

Ceci est confirmé par une analyse sommaire du développement des techniques de surveillance, qui se sont développées dans une première phase, notamment à partir des années 70, dans la surveillance de la circulation routière ou bien pour prévenir les vols et les braquages dans les banques et les magasins de luxe.

Des liens importants entre la surveillance et les droits individuels avaient déjà été néanmoins signalés, en particulier dans les relations de travail, au point que certains pays ont été conduits à interdire ou réglementer spécifiquement l'usage de techniques audiovisuelles et d'autres outils, dans la mesure où ceux-ci étaient employés pour des finalités de contrôle à distance des employés (v. par exemple la loi italienne n° 300 de 1970).

Dans les années suivantes, le lieu du travail a été celui dans lequel les techniques de surveillance ont été développées le plus, puisque ceci a permis de mieux contrôler la sécurité des installations, la qualité et la régularité des prestations et la productivité. Il fut aussi dès-lors possible de contrôler des comportements et des situations sans rapport avec une évaluation professionnelle.

Les années 80 ont connu aussi une augmentation de l'usage de techniques de surveillance dans le domaine des transports (en particulier dans les métros et dans les environs), ainsi qu'à l'intérieur de certains bâtiments publics (afin de prévenir des actes de vandalisme) ou dans des établissements de loisir.

Leur utilisation croissante dans un nombre croissant d'établissements commerciaux grand public a facilité les analyses sur les réflexes et les habitudes des consommateurs par rapport aux modalités d'étalage des marchandises exposées pour la vente. Dans ce secteur, les systèmes de surveillance (vidéo en particulier) sont devenus un instrument précieux pour des finalités commerciales (même si au début ou en apparence ils ont été déployés pour la prévention des vols et du vandalisme) et ont ouvert la possibilité de rationaliser les ressources de l'entreprise à l'intérieur d'un même établissement (par exemple: détermination du nombre et des horaires d'ouverture des caisses et contrôle des accès, et de manière plus générale, création de "parcours d'achat" visés à stimuler les consommateurs).

Les techniques de surveillance ont connu une évolution ininterrompue qui s'est étendue aux secteurs les plus divers.

Dans le domaine de la circulation, les endroits contrôlés ont augmenté sans cesse, dans les routes et autoroutes, pour des finalités de contrôle de la circulation, des infractions (même par le biais de systèmes infrarouge) et, plus récemment, des accès au centre de villes grandes et petites.

Par exemple, des appareils de contrôle vidéo ont été installés dans des :

- stades et installations sportives Footnote 1 ;

- stations à essence;

- casinos;

- établissements de santé (en particulier dans les unités d'urgence, soins intensifs, interventions chirurgicales);

- installations de traitement des eaux usagées et de déchets.

Ce développement concerne aussi musées, cathédrales, ainsi que l'observation par satellite du territoire (pour des finalités de prises d'images périodiques ou géographiques, de gestion du trafic aérien ou urbanistiques).

Des techniques semblables de contrôle à distance, basées sur la transmission de signaux, sont utilisées pour le bracelet électronique appliqué à des personnes en liberté surveillée, semi-liberté, congé pénitentiaire etc.

Des utilisations plus récentes commencent à se manifester aussi dans les secteurs suivants:

- prévention de l'immigration irrégulière;

- sécurité d'unités immobilières et de lotissements locatifs (avec la tendance significative à créer, en milieu industriel et commercial, des zones "forteresses" protégées à l'égard de comportements illicites tels que vols, cambriolages, vandalisme);

- transports en commun (des actions pilotes dans les taxis de New York sont basées sur la prise d'images à infrarouge au moment où le client monte dans la voiture ou lorsque le taximètre est activé, enregistrées sur support digital et effacées automatiquement sauf si le chauffeur ou le propriétaire en décide autrement);

- web-cams ou caméras en lignes utilisées pour diffuser des images pour des finalités de promotion touristique ou de publicité de certains établissements ouverts au public tels que bistrots, boites de nuit et même de démonstration au public du niveau de vie dans les prisons;

- banques, dans l'entrée desquelles l'on installe des dispositifs occultes de détection des empreintes digitales et, en même temps, d'une image photographique, de manière à pouvoir identifier en vidéo et avec empreinte tous les visiteurs, clients habituels ou pas, parmi lesquels peuvent se cacher des cambrioleurs ou des complices chargés d'explorer les lieux.

En outre, il y a lieu de souligner le recours volontaire à des techniques de contrôle à distance pour la gestion de ladite "*e-family*", et la théorisation de recherches statistiques sur image visant à définir des comportements-type des membres de certaines communautés/groupes.

Finalement, il y a lieu de considérer les connections de ce problème avec les intérêts économiques liés à la production de tels instruments, à la réduction des primes

d’assurance offerte à ceux qui installent des systèmes de surveillance ou des systèmes d’antivol satellitaires sur les voitures assurées.

2) QUELQUES MOTS SUR LES TECHNIQUES DISPONIBLES

Comme déjà dit plus haut, l’évolution croissante des techniques impose de situer dans son contexte le thème de la surveillance.

Le développement technique des systèmes a tout d’abord mis en lumière, tour à tour, la possibilité de:

- transmettre des images vers un « centre » depuis des terminaux par câble, fibres optiques ou réseaux digitaux ;

- enregistrer les images qui sont, dans un premier temps, simplement visualisées par le biais d’un CCTV – télévision à circuit fermé ;

- obtenir des images ayant un meilleur niveau de définition des reproductions couleur ;

- associer images et sons ;

- augmenter le champ visuel jusqu’à 360° ;

- disposer de caméras fixes et/ou mobiles, stationnaires et/ou rotatives ;

- disposer de la fonction zoom et donc de la possibilité d’agrandir des segments significatifs de l’image prise.

Tout inventaire dans cette matière risquerait donc d’être vite dépassé.

En respectant les proportions, le tournant le plus significatif a été enregistré non pas tellement dans l’évolution des techniques de transmission (exemple : émetteurs sous-cutanés utilisés en cas de surveillance alternative à la détention) ou dans le passage de la simple visualisation d’images à leur enregistrement et leur conservation, mais bien dans le fait d’y ajouter des systèmes intelligents d’analyse et d’intervention. Footnote 2

En effet, les systèmes les plus récents ne se bornent pas à prévoir la fonction d’arrêt sur image (et, le cas échéant, de leur impression), ni à être reliables à un « centre » qui peut lancer des signaux d’alarme sonore ou visuelle, ou bien déterminer le blocage des points d’entrée ou de sortie de certains endroits ou établissements, ou l’intervention du personnel et même d’hélicoptères d’urgence. Ces systèmes peuvent aussi incorporer - ou être associés à - des logiciels pour la recherche automatisée d’images. Certains systèmes permettent la reconnaissance de personnes recherchées par des techniques de « ciblage de criminels présumés », par exemple sur la base de la reconnaissance automatique du visage – *Facial mapping computer*.

L’on assiste de plus en plus à la réalisation de systèmes permettant de lancer des alarmes de nature variée (à partir de la simple signalisation au personnel de vigilance) à l’égard de personnes suspectes sur la seule base de clichés ou bien de personnes qui

adoptent un comportement que le système reconnaît automatiquement comme « anormal » (par exemple, dans un parking ou à l'entrée d'un stade).

L'on peut préfigurer ainsi la possibilité de détecter dans le futur des anomalies présumées de comportement, découlant de simples signes extérieurs (traits somatiques, vêtements, couleur de la peau) ou d'actes ou faits encodés au préalable comme étant intéressants (mouvements brusques, fumée, ouverture de portes).

Tandis que dans le passé on assistait, entre hypermarchés, à des échanges de vidéocassettes reprenant les images de consommateurs « suspects » ou déjà surpris sur le fait, les systèmes plus sophistiqués peuvent désormais identifier voix et conversations ou tout au moins des mots-clé ou bien rechercher une voix ou un visage dans le cadre d'une liste indexée. Par exemple, en 1998 une expérience pilote a permis d'examiner en temps réel plus de 1000 images par seconde afin de retrouver un visage déterminé, sans que le système puisse être « trompé » par une barbe ou des moustaches utilisées par la personne concernée afin de cacher son image.

D'autres expériences récentes permettent aussi de tracer le parcours présumé suivi par une personne ou un véhicule dans le cadre de scénarios complexes ou d'identifier des personnes qui suivent un même parcours souvent ou périodiquement.

Toutes ces techniques peuvent évidemment être utilisées non seulement pour la prévention et la répression de délits, mais aussi pour d'autres finalités, comme par exemple la recherche de personnes ou mineurs disparus ou pour des finalités d'intérêt public qui ont amené le Conseil de l'Europe même à en recommander dans certains cas l'utilisation. Footnote 3

Des systèmes de reconnaissance du visage ont été utilisés même pour prévenir des faux mariages, ou bien, sur une base consensuelle, pour permettre l'accès au lieu du travail ou à des immeubles (sur la base, par exemple, d'une programmation de l'ouverture automatique des portes aux membres d'une même famille) ou bien pour acheter des tickets d'avion ou pour utiliser des terminaux ATM (*automated teller machines* ou guichets automatiques).

L'évolution technique est, à cet égard, constante. Footnote 4

3) SYNTHESE DES EFFETS DE LA SURVEILLANCE

La mise en contexte susmentionnée conditionne aussi l'analyse des effets de la surveillance.

En règle générale, l'analyse intervient en retard sans être connue par le grand public et est le fait exclusif de quelques experts. Au moment où, par la suite, cette analyse devient publique, la technique a cependant évolué et exige de nouvelles réflexions et analyses. Footnote 5

A ce jour, par exemple, les techniques de reconnaissance du visage ne sont pas encore tellement répandues et, en parallèle, les réflexions susmentionnées sont conduites seulement par une doctrine éclairée ou par quelques articles de presse. Entre-temps, la diffusion croissante des techniques de surveillance et l'augmentation du nombre des

personnes disposant d'images nécessitera un nouveau type d'analyse, plus avancé. Par exemple, il est temps que la doctrine et les juristes ne se bornent pas à souligner les risques de la surveillance, mais considèrent avec plus d'attention le problème de l'interconnexion en temps réel des images de surveillance détenues par différentes entités (autoroutes, banques, conseils municipaux etc.).

Ceci dit, la question des incidences de la surveillance ne devrait pas être un sujet réservé aux juristes car le développement des mécanismes de contrôle dans le domaine public rend nécessaire une évaluation politique de la part des institutions compétentes et des Parlements.

Le sujet impose tout d'abord une évaluation de la proportionnalité en ce qui concerne le rapport entre les exigences de sécurité et la protection de la vie privée.

En effet, les systèmes de surveillance peuvent produire certains effets positifs sur le plan de la sécurité. Le degré de ces effets n'est toutefois pas uniforme. Quelques applications ont produit une baisse certaine des actes illicites dans les espaces publics. D'autres se sont néanmoins montrées inefficaces ou ont déplacé la criminalité vers des zones limitrophes ou se sont limitées à offrir des éléments de preuve à l'encontre de personnes observées.

En deuxième lieu, il faut considérer que les systèmes de reconnaissance somatique ou comportementale peuvent comporter souvent des erreurs au détriment d'innocents spectateurs, étant basés sur la réduction des visages à quelques dizaines d'« éléments constitutifs » et sur le calcul de distances entre les « parties clé ».

La possibilité que les systèmes de surveillance fassent tache d'huile comporte aussi le risque d'une banalisation qui pourrait réduire leurs effets positifs. Finalement, l'on risque de recourir de manière excessive à la surveillance non pas tellement pour satisfaire des exigences objectives (dans une ville italienne, l'on a par exemple envisagé un système de vidéosurveillance de certaines rues du centre ville car les patrouilles de police en voiture n'arrivent pas à visualiser certains endroits, tels que des galeries) mais bien comme solution expéditive à des carences structurelles ou organisationnelles des activités de police.

Enfin, l'on est arrivé jusqu'à théoriser une distinction entre :

- une surveillance répressive (visant à permettre d'intervenir en cas de comportements indésirables) et

- une surveillance préventive (visant à établir une relation avec les citoyens afin de les pousser à suivre certains comportements standard).

En d'autres termes, il y a lieu de craindre que la tendance de la société contemporaine ne soit de remplacer - ou de compléter - la répression par l'incitation à l'autocontrôle et la répression des impulsions.

Cette considération impose de développer la réflexion sur la surveillance, qui souvent se borne à analyser la question de savoir si les mécanismes de contrôle lèsent des

libertés individuelles d'une manière disproportionnée par rapport aux exigences de prévention et de répression des délits. Footnote 6

A cet égard, il n'y a pas de doutes sur la nécessité d'une approche beaucoup plus sélective dans l'utilisation future des systèmes de surveillance, l'impératif étant d'éviter que la masse des citoyens ne soit soumise à des limitations excessives pour prévenir des comportements qui, s'ils sont certes dommageables, demeurent le fait de minorités.

Le débat devrait donc être enrichi en dépassant le thème des effets positifs sur la sécurité des biens et des personnes, et analyser aussi les effets potentiels sur les libertés et les comportements des citoyens.

En d'autres termes, au-delà de la réflexion sur le degré de violation de la vie privée, deux questions se posent en relation aux effets qu'un recours massif à la surveillance de la part de plusieurs sujets peut comporter :

- sur la liberté de circulation des citoyens ;

- sur leurs comportements.

Sous le premier angle, il faut s'interroger sur la question de savoir si la liberté de circulation, reconnue par plusieurs chartes constitutionnelles et par l'article 2 du protocole n° 4 additionnel à la Convention européenne des droits de l'homme, recouvre une liberté de circulation exclusivement formelle, ou substantielle aussi, c'est à dire la liberté de circuler sans devoir laisser des traces constantes ou fréquentes des ses mouvements à des systèmes de « délation optique » permanente.

En ce qui concerne le deuxième aspect, le fait «d'être vu sans voir » peut conditionner le comportement et les activités d'une personne. D'une part, les installations occultes de prise de vue ou de contrôle n'encouragent pas la transparence pour le citoyen. De l'autre, les caméras ou autres dispositifs dont l'installation est connue au citoyen pourrait, dit-on, dans certaines circonstances, mener à des comportements de « soumission ».

S'il est vrai que dans les espaces publics l'on peut s'attendre à une moindre protection de la vie privée, on doit néanmoins rejeter la théorie selon laquelle il n'y aurait point de protection de la vie privée dans les espaces publics.

A cet égard, il suffit de penser :

- aux dispositions nationales en matière de droit d'auteur non-patrimonial, qui reconnaissent une certaine protection à l'égard de la diffusion d'images liées à des faits, des événements, des manifestations publiques ou d'intérêt public ;

- aux dispositions nationales qui, transposant la directive européenne 95/46/CE, reconnaissent à la personne concernée le droit de s'opposer pour des raisons légitimes au traitement de ses données à caractère personnel, même si le traitement est en soit légitime.

De plus, il doit être noté que l'exigence de transparence est parfois remplie uniquement par la notification du fait de l'installation et du fonctionnement de caméras ou d'autres moyens de contrôle à distance. Ainsi, des citoyens sont tenus de fournir des données à caractère personnel (qui consistent souvent en des images) ; ils ne sont toutefois pas informés sur l'utilisation de ces données, quand bien même ces données ou ces images seraient inclues dans des fichiers ou utilisées à des fins d'identification. Les citoyens peuvent être ainsi réduits à des « objets » d'informations, sans égard au droit à l'autodétermination informationnelle. Footnote 7

Le manque de transparence prive le citoyen du droit de savoir que certains éléments de preuve, représentés par des données ou des images, peuvent être utilisés de manière à lui porter préjudice.

Si le souci de discriminations possibles à l'égard de minorités ou de personnes ayant une certaine orientation sexuelle peuvent sembler excessives à certains, dans les sociétés démocratiques modernes, le risque d'un contrôle envahissant et omniprésent est réel, et la technologie ne doit pas rendre impossible le maintien d'espaces d'anonymat ou d'intimité, *a fortiori* lorsque la reproduction d'images est effectuée pour des finalités privées ou de moindre intérêt public (que l'on pense aux récentes expériences de caméras web publicitaires de plages et établissements balnéaires, qui effectuent des prises d'image régulières et rapprochées des personnes qui n'en sont pas informées).

4) LES INSTRUMENTS ADOPTES A CE JOUR PAR LE CONSEIL DE L'EUROPE

Il n'est probablement pas nécessaire de rappeler ici que les principes de la Convention n° 108/1981 s'inspirent des dispositions de la Convention européenne des droits de l'homme, Footnote 8 de même, il va de soi que le traitement des données à caractère personnel, concernant des personnes physiques, collectées dans le cadre d'activités de surveillance, tombe normalement dans le champ d'application de la Convention 108.

En effet, pour les instruments utilisés (ex. : caméras, ordinateurs, écouteurs, satellites, systèmes GPS), ce type de traitement est effectué en partie à l'aide de procédés automatisés (art. 2, c de la Convention 108).

Pour les Parties contractantes qui, comme l'Italie, ont utilisé la faculté d'appliquer la Convention aux traitements des données concernant les groupes, associations, fondations, sociétés, etc. et aux traitements non automatisés (art. 3 b et c de la Convention), les garanties de la Convention s'appliquent, bien entendu, dans ce domaine aussi.

En vertu de l'article 11 de la Convention 108, certaines Parties contractantes ont appliqué aussi ces garanties à la collecte, conformément à la directive 95/46/CE qui, à la différence de la Convention, inclut la collecte dans la notion de « traitement ».

Ceci implique que, sous réserve des dérogations éventuelles prévues par le droit interne dans les limites de l'art. 9 de la Convention, le traitement des données pour des finalités de surveillance est soumis, en particulier, aux articles 5 (qualité des

données), 7 (sécurité), 8 (droit d'accès), 10 (sanctions et recours) et 12 (flux transfrontaliers).

L'application de ces dispositions à la surveillance soulève un certain nombre de réflexions qui seront développés à propos d'autres initiatives qui pourraient être prises par le Conseil de l'Europe.

Il importe néanmoins de souligner d'ores et déjà que l'art. 5, appliqué à la surveillance, impose à celui qui traite les données une série d'obligations qui (dans la mesure où le droit interne couvre aussi la collecte et que les opérateurs respectent cet article de manière rigoureuse) ont un impact important sur les modalités techniques de collecte des données. A titre d'exemple, on peut songer à l'orientation et au champ visuel des caméras, au spectre des micros, au choix d'enregistrer les données au pas, etc.

En ce qui concerne l'art. 6 de la Convention 108, il y a lieu de remarquer que certaines données collectées aux fins de surveillance ne rentrent sûrement pas dans le champ d'application de la disposition (exemple : surveillance pour certaines finalités commerciales ou surveillance des apprentis du marketing direct ou encore certaines activités de surveillance effectuées par des détectives privés en relation avec des litiges en matière civile etc.). D'autres catégories de données, par contre, y rentrent sans aucun doute (exemples : surveillance dans les salles de chirurgie ou de premiers secours des hôpitaux ou pour des actions ciblées de surveillance des manifestations politiques ou syndicales par la police, surveillance dans des endroits où résident des minorités ethniques ou encore en relation avec la prostitution, etc.)

L'on discute en revanche de savoir si l'art. 6 s'applique aussi aux données collectées, en particulier par la police, sur des criminels présumés, pas encore condamnés. Si la lecture textuelle de l'art. 6, deuxième alinéa, peut amener à conclure pour la négative, puisque celui-ci se réfère uniquement aux condamnations pénales, il faut néanmoins considérer que, de l'avis de certains experts, « les données liées à une infraction, même lorsqu'il n'y a pas encore de condamnation pénale mais simplement une suspicion » devraient être considérées comme des données sensibles Footnote 9.

Bien qu'en application de l'art. 11, les Parties contractantes peuvent étendre la protection des données sensibles, la question interprétative est importante puisque, pour le traitement des données sensibles ou assimilées à des données sensibles sur la base de l'art. 6, il est nécessaire que la loi ou bien des règlements ou encore des directives administratives (Footnote 10) prévoient des garanties appropriées, tandis que les dérogations éventuelles aux principes de la Convention, au sens de l'art. 9, doivent nécessairement être introduites par un acte législatif, en prenant en compte le principe de « nécessité » tel qu'élaboré par la Cour européenne des droits de l'homme. Footnote 11

Pour conclure ce court aperçu sur la Convention, il faut aussi rappeler ce qui suit :

- les Parties contractantes peuvent exclure du champ d'application de la Convention certains traitements des données, par exemple pour les traitements des données en matière de sauvegarde de la sécurité de l'Etat (comme déclaré par l'Irlande) ou les traitements pour utilisation purement privée ou domestique (exclus par plusieurs Parties) ;

- les données et informations collectées dans le cadre d'une surveillance sont soumis à la Convention dans la mesure où elles se rapportent à une personne identifiée ou identifiable par le biais de liens avec d'autres informations (indépendamment du fait que l'information concerne des données linguistiques, des images statiques ou dynamiques ou encore des sons). A cet égard, le Comité Consultatif de la Convention 108 a rejeté l'avis selon lequel les voix et les images ne sont pas considérés comme des données à caractère personnel si elles ne sont pas accompagnées d'informations nominatives. En réalité, il suffit que les voix ou les images fournissent des informations sur une personne en la rendant identifiable même de manière indirecte. Footnote 12

5) NOTION DE SURVEILLANCE PRISE EN CONSIDERATION

La notion de surveillance est en soi très large et dépasse le thème du contrôle par des équipements vidéo (bien que ce dernier représente une partie significative de cette réalité), puisqu'elle peut inclure aussi le contrôle de conversations téléphoniques et télématiques, ainsi que de la circulation de documents. Elle peut inclure aussi le contrôle à distance de certains usagers d'un service (ex. : localisation des terminaux de téléphonie mobile) ou de personnes en relation avec une action en justice (ex. : bracelet électronique).

Par conséquent, l'objectif de prendre en compte dans une seule recommandation ou un document de « lignes directrices» le sujet de la surveillance dans son ensemble est certainement louable, mais très ambitieux et source de difficultés potentielles dans la rédaction du texte et dans son application.

A titre d'exemple, que l'on pense aux problèmes spécifiques de la surveillance utilisée pour faire valoir un droit en justice, de même qu'aux dérogations au droit d'accès qui, dans ce cas, devraient être limitées dans le temps et dans leur étendue.

Que l'on pense aussi à la surveillance de la correspondance des détenus (courrier papier et électronique), thème sur lequel la Cour européenne des droits de l'homme s'est dernièrement prononcée le 28 septembre 2000 par un arrêt non définitif qui soulève des réflexions complémentaires sur le problème de la base juridique (Deuxième section – Affaire M. c. Italie, Requête n. 25498/94).

Le Groupe de projet sur la protection des données du Conseil de l'Europe travaille beaucoup et fait appel à des experts hautement qualifiés dans le but d'enrichir les instruments déjà élaborés par le Conseil en y intégrant des dispositions qui se rapportent aussi aux innovations techniques.

Un objectif si important impose une approche extrêmement rigoureuse afin de :

- éviter chevauchements, contradictions éventuelles, manque de coordination et atténuations indésirables de garanties par rapport à certaines dispositions inclues dans les recommandations du Conseil de l'Europe existantes ; et

- éviter de suivre une approche trop abstraite pour « couvrir » tout type de surveillance existant au sens large du terme ; avec le double risque d'édicter des dispositions typiques, par exemple, pour la vidéo-surveillance mais difficilement applicables à

d’autres secteurs ou de ne pas prévoir des règles ou exceptions qui elles seraient en revanche nécessaires à un niveau plus spécifique.

L’ensemble des recommandations existantes du Conseil de l’Europe applicables en la matière offre un cadre incomplet de garanties en matière de surveillance, mais ce cadre ne doit pas être affaibli, notamment en ce qui concerne le champ d’application.

A) Par exemple, par rapport à la Recommandation n° R (87) 15, il serait souhaitable de ne pas omettre de prendre en compte, dans une initiative future du Conseil de l’Europe, les activités menées par la police dans le cadre d’une enquête spécifique prévue par la loi, ainsi que les activités d’une agence de renseignement de sécurité ou militaire.

Quant aux enquêtes spécifiques, tout en tenant compte de la diversité des systèmes juridiques, on doit prendre en considération la possibilité de permettre des exemptions dans le cadre des règles de procédure pénale, uniquement si elles sont liées à la commission d'une infraction pénale.

Le Préambule de la Recommandation n° R (87) 15 prévoit qu'un Etat membre a la faculté d'étendre les principes au traitement des données à des fins de sécurité de l'Etat. Il est possible de prévoir cette même possibilité dans toute nouvelle initiative du Conseil de l’Europe, sous réserve de garanties appropriées.

S'agissant de la prévention et de la lutte contre la criminalité ainsi que de la protection de l'ordre public, il conviendrait d’essayer d’éviter l’application simultanée de la Recommandation R(87)15 et d’un nouvel « instrument » élaboré par le Conseil de l’Europe. La Recommandation R(87)15 contient d’ailleurs des dispositions importantes qui devraient être dûment prises en compte dans le cadre de futures initiatives.

Ainsi, selon la Recommandation R(87)15 :

a) l'introduction de nouveaux moyens techniques pour le traitement de données ne devrait être admise que si toutes les mesures raisonnables ont été prises pour s'assurer que leur utilisation est conforme à l'esprit de la législation existante sur la protection des données (principe 1.2) ;

b) la collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger *concret* ou à la répression d'une infraction pénale *déterminée*. Toute exception à cette disposition devrait faire l'objet d'une législation nationale spécifique (principe 2. 1) ;

c) la collecte de données par le biais de moyens techniques de surveillance ou d'autres moyens automatisés devrait être prévue dans des dispositions *spécifiques* (principe 2.3).

d) la collecte de données sur des individus pour le seul motif de leur origine raciale, de leurs convictions religieuses, de leur comportement sexuel ou de leurs opinions politiques, devrait être prohibée (principe 2.4);

e) les cas dans lesquels les données peuvent être communiquées sont énumérés (principe 5), ce qui rend difficile la définition de mesures supplémentaires en la matière.

Enfin, il conviendrait de prendre en considération la disposition de la Recommandation R(87)15 selon laquelle, lorsque des données concernant une personne ont été collectées et enregistrées à son insu, cette personne devrait en être informée, si les données ne sont pas détruites (principe 2.2). Cela est particulièrement important dans le cadre des propositions tendant à limiter éventuellement le droit, pour la personne concernée, d'être informée des activités de surveillance dont elle fait l'objet, si ces limites sont prévues par la loi et visent à éviter que les activités de surveillance ne soient entravées.

B) Quant à la Recommandation (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi, on pourrait examiner en particulier la disposition exigeant que les salariés soient informés ou consultés avant l'introduction de systèmes automatisés pour la collecte des données et leur utilisation (principe 3.1) - en plus de la disposition générale sur le respect de la vie privée et de la dignité humaine des travailleurs, en particulier quant à leur possibilité d'avoir des relations sociales et personnelles sur le lieu de travail (principe 2). Cette disposition s'applique aussi à l'utilisation des postes de téléphone à ligne directe sur le lieu de travail (Recommandation R(95)4, principe 7.15).

Il conviendrait d'accorder une attention particulière aux dispositions concernant la collecte et le stockage de données « sensibles » sur les travailleurs (voir. Principe 10.1 de la Recommandation R(89) 2).

C) Il conviendrait d'éviter des chevauchements avec la Recommandation (95) 4 sur la protection des données à caractère personnel dans le secteur des télécommunications, en particulier en ce qui concerne les services téléphoniques. En effet, cette Recommandation régit aussi les services fournis par les réseaux qui autorisent les utilisateurs à correspondre à travers des images. À cet égard, elle prévoit que des systèmes anonymes d'accès aux réseaux soient mis en place et que toute interférence dans le contenu de la communication soit en principe interdite (principes 2.2, 2.3, 2.4 et 2.5). Quant à la facturation pour l'utilisation des services téléphoniques, l'abonné ou la personne appelée doit avoir la garantie de ne pas pouvoir être localisé de manière précise (principe 7.2.1).

D) D'autres recommandations contiennent des dispositions générales en matière de traitement des données qui, même si elles ne se réfèrent pas explicitement à la surveillance, portent néanmoins des garanties et des règles qui lui sont applicables et doivent donc être coordonnées, notamment en matière de communication des données et de transfert transfrontalier de données.

Si le Conseil de l'Europe maintient l'objectif ambitieux d'élaborer des normes applicables à la surveillance dans son ensemble ou à certains types de surveillance – et notamment à la vidéo-surveillance -, une coordination avec certaines recommandations existantes est nécessaire. Ceci pourrait se faire selon l'une des alternatives suivantes :

- en évitant les cas de chevauchement et en déclarant que toute nouvelle initiative du Conseil de l'Europe (des lignes directrices sur la surveillance, par exemple) ne vise qu'à compléter les recommandations précédentes et s'applique uniquement aux questions qui ne sont pas traitées dans ces recommandations, dont le contenu serait donc sauvegardé. Cette réduction pourrait, toutefois, ne pas être tout à fait satisfaisante, puisque quelques recommandations seulement contiennent déjà des dispositions applicables à cette matière, même indirectement et que l'on risquerait donc d'exclure certains secteurs de l'application des dispositions pertinentes existantes ;

- en harmonisant pleinement le contenu de toute nouvelle initiative du Conseil de l'Europe avec celui des recommandations existantes et en indiquant que ces dernières seraient en substance enrichies et précisées (par exemple, en ce qui concerne les modalités de collecte des données, d'exercice des droits de la personne concernée, etc.).

Il serait également envisageable d'évaluer la possibilité d'approuver une liste de lignes directrices, un «décalogue » plus synthétique, ciblé de manière plus spécifique sur la vidéo-surveillance et visant seulement à introduire des garanties supplémentaires qui ne se chevaucheraient pas avec les garanties existantes.

Quelle que soit la solution retenue, le Conseil de l'Europe pourrait parvenir rapidement à une solution satisfaisante en complétant l'analyse déjà menée sur le thème de la surveillance.

Dans ce but, j'estime qu'il pourrait être utile d'examiner les ébauches de propositions figurant ci-après, qui ne sont nullement exhaustives.

6) REMARQUES GENERALES

Premièrement, il faut être conscient du risque d'élaborer un instrument dont le champ d'application serait excessivement étendu : dans un tel instrument, il serait difficile de tenir compte, simultanément et dûment, de toutes les exigences et – surtout – de toutes les exceptions, et d'envisager tous les cas où des activités de surveillance sont organisées et tous les objectifs qu'elles poursuivent, sans introduire d'incohérences ni affaiblir la protection. Footnote 13

Deuxièmement, il faut essayer d'éviter qu'une nouvelle initiative du Conseil de l'Europe dans ce secteur puisse être jugée – en raison de son champ d'application étendu – trop générique et trop peu novatrice, puisqu'elle ne comporterait pas les lignes directrices requises par les dispositions s'appliquant à la collecte et au traitement des données aux fins de surveillance (renforcer le principe de finalité et proportionnalité ; modalités spécifiques pour le droit d'accès ; règles sur l'indexation des données et sur l'interconnexion des systèmes ; règles plus spécifiques sur la conservation ; l'interdiction des traitements automatisés visant à définir la personnalité, etc.).

7) DEFINITIONS

La notion de surveillance pourrait être définie comme : *« toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte et/ou l'enregistrement de manière non occasionnelle des données de caractère personnel d'une ou plus personnes, relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés »* si le Conseil de l'Europe décide de ne pas se limiter à la vidéo-surveillance *(Footnote 14)*. En effet, il y a des raisons pour préférer une définition large qui ne rentre pas dans des détails techniques excessifs. En outre, il serait préférable de faire référence à une surveillance non occasionnelle plutôt qu'à des opérations « systématiques ». De plus, les activités de surveillance devraient être envisagées en tant que telles, qu'elles risquent ou non de constituer une ingérence dans la vie privée.

Il y a lieu peut-être de rappeler explicitement que les images et les sons sont aussi considérées comme des données à caractère personnel (lorsque les équipements concernés permettent d'identifier même indirectement les personnes concernées) ainsi que les données de trafic ou celles découlant de la transmission d'impulsions (signaux), qui permettent de localiser les personnes ou de déterminer le moment et les interlocuteurs de communications ou conversations données.

La définition de « traitement », si elle est donnée, doit clarifier le fait que l'on s'adresse aussi à la simple observation de comportements, sans enregistrement (à moins que l'on considère que l'observation est incluse dans la notion de collecte).

Il faudrait s'interroger sur la question de savoir s'il faut distinguer la notion de communication de celle de diffusion.

Il faudrait évaluer l'opportunité de clarifier que pour certains types de surveillance, en présence d'une information claire et efficace, le comportement concluant et non ambigu de la personne intéressée peut être assimilé au consentement.

Tout en admettant l'exclusion des activités de surveillance consistant en des traitements de données dans le cadre de la vie privée ou familiale du champ d'application de tout nouvel instrument (précision qui est en partie superflue compte tenu du fait que plusieurs Parties ont exclu cet aspect du champ d'application de la Convention), il serait peut-être moins approprié d'exclure totalement les activités suivantes :

- les activités de surveillance effectuées par les autorités de police dans le cadre d'enquêtes spécifiques prévues par la loi ; de fait, il serait préférable de faire référence aux activités menées dans le cadre d'enquêtes pénales, qui dans certains pays peuvent être effectuées directement par des magistrats, plutôt que par des policiers, en application des dispositions nationales régissant la procédure pénale ;

- les activités de surveillance effectuées par les organes chargés d'assurer la sûreté de l'Etat ; ainsi, toute exception concernant la sûreté de l'Etat devrait être coordonnée avec la faculté – reconnue aux Parties par la Recommandation n° R(87)15 – d'appliquer à cet égard cette dernière recommandation ;

- les activités journalistiques : la collecte de données en liaison avec la liberté d'expression ne doit pas être l'occasion d'exercer une surveillance sans limites – compte tenu notamment des dispositions prises dans divers pays européens à la suite de la directive 95/46/CE.

8) RESPECT DE LA VIE PRIVÉE

Il paraît indiqué de mentionner brièvement, dans tout nouvel instrument élaboré par le Conseil de l'Europe, la nécessité d'appliquer les dispositions nationales relatives à la vidéosurveillance en prenant en compte les garanties constitutionnelles ainsi que les dispositions du Code pénal relatives à la protection du domicile, en vertu desquelles certains lieux tels que les chambres d'hôtels, les bureaux, les toilettes publiques, les vestiaires, les points phone sont considérés comme des « domiciles » (Footnote 15). Il faut signaler ici que le code de procédure pénale de certains pays rend totalement irrecevables les éléments de preuve collectés en violation de la loi (Footnote 16).

Il conviendrait de s'interroger sur l'opportunité d'appeler les Etats membres, les fabricants, les fournisseurs de services et d'accès ainsi que les chercheurs à s'engager à porter une plus grande attention, lors du développement des logiciels, des technologies et des dispositifs techniques, aux droits fondamentaux des personnes concernées (Footnote 17). Des suggestions analogues figurent par exemple :

- dans la Recommandation n° 1/99 sur les opérations invisibles de traitement des données sur l'Internet, telle qu'adoptée le 23 février 1999 par le Groupe de travail des autorités de contrôle de la protection des données des Etats membres de l'Union européenne, établi en application de l'article 29 de la Directive 95/46/CE (cette recommandation s'applique aussi, entre autres, aux « *clickstreams* ») ;

- de manière plus marginale, dans la Recommandation n° R(99)5 du Conseil de l'Europe sur la protection de la vie privée sur Internet (voir le préambule, qui invite à développer des technologies permettant de préserver l'anonymat des personnes concernées) Footnote 18 et dans la directive 97/66/CE concernant la protection de la vie privée dans le secteur des télécommunications (qui encourage, par exemple, la mise au point de nouvelles formes d'accès anonyme et strictement confidentiel aux services de télécommunications publics, voir le considérant n° 18).

En revanche, il ne semble pas nécessaire d'aborder un autre point, régi par le droit public et civil, à savoir les cas dans lesquels le propriétaire d'un lieu est tenu, par un organisme public, un particulier ou une copropriété, de faire installer des systèmes de surveillance permanente.

9) COLLECTE ET TRAITEMENT DES DONNÉES RELATIVES À LA SURVEILLANCE

Il pourrait être utile de réaffirmer et de souligner les principes selon lesquels, les données à caractère personnel devraient être traitées de manière loyale et licite, et pour des finalités légitimes, spécifiques et explicites.

10) CRITÈRES DE LICÉITÉ

Lors de la définition des critères de licéité s'appliquant à la surveillance ou à la vidéo-surveillance, il conviendra de prendre en compte les garanties déjà prévues par le second principe de la Recommandation n° R(87)15 (existence d'une législation spécifique, prévention d'un danger concret).

De plus, ces critères devront être adaptés à d'autres cas de figure, comme la surveillance mise en place par un avocat ou par un détective privé dûment mandaté par la défense dans une affaire judiciaire ou encore pour la surveillance d'apprentis en marketing direct.

Pour ce qui est du degré de précision de la législation nationale, l'arrêt rendu le 4 mai 2000 par la Cour européenne des Droits de l'Homme dans l'affaire *Rotaru c. Roumanie* - en même temps que la 5e réunion du CJ-PD-GC (10 au 12 mai 2000) - devrait être dûment pris en considération (Footnote 19).

Des adaptations devront aussi être envisagées pour ce qui est de la surveillance à des fins médicales (protection de la vie, de l'intégrité physique ou de tout autre intérêt légitime de la personne concernée ou d'un tiers). Une attention particulière devra être accordée aux cas dans lesquels la surveillance peut être prévue par la loi. Cependant, ni la personne concernée, ni la tierce personne ne sont en mesure d'exprimer leur consentement. Il est fait allusion ici à des cas survenus en Italie, concernant la surveillance continue de personnes dans le coma ou en soins intensifs ou encore à des personnes hospitalisées dans un service de quarantaine et que leurs proches ne pouvaient voir qu'à distance, et où d'autres malades auraient pu être vus si des mesures appropriées n'avaient pas été prises.

Enfin, je suggérerais de compléter les critères de licéité pourraient être complétés par des dispositions de protection des personnes concernées contre des « décisions individuelles automatisées » concernant leur personnalité, leurs performances professionnelles, leur fiabilité, leur comportement, leur origine ethnique, etc., découlant « automatiquement » du traitement de données collectées à des fins de surveillance (voir l'article 15 de la Directive 95/46/CE) ; citons simplement à titre d'exemple le déclenchement de signaux d'alarmes fondés sur des techniques de reconnaissance faciale en fonction de la couleur de la peau).

Je tiens en outre à appeler l'attention du Conseil de l'Europe sur les lois et réglementations nationales imposant l'enregistrement du contenu ou des données de trafic, permettant l'identification des appels téléphoniques et des messages transmis par voie électronique qui concernent des transactions boursières.

11) FINALITE

Tout instrument qui laisserait la voie ouverte au contrôle à distance de l'efficacité des salariés - interdit dans de nombreux pays – serait inacceptable. Ce point doit être formulé beaucoup plus clairement par le Conseil de l'Europe : il faut interdire complètement tous les systèmes visant à déterminer la productivité des employés et la qualité de leur travail. Par contre, les systèmes servant plusieurs objectifs — et répondant par exemple à des impératifs d'organisation, de production ou de sécurité

du travail — peuvent être tolérés, comme c'est le cas dans certains pays. L'utilisation de ces systèmes pouvant se traduire par un contrôle à distance des employés, il conviendra toutefois, dans cette éventualité, d'insister sur le respect des droits syndicaux. Du reste, dans certains pays, ce type de systèmes de surveillance ne peut être installé qu'après information préalable des syndicats concernés, et même, dans certains cas, avec leur accord.

A cet égard, des garanties devraient être prévues pour toutes les données, qu'elles soient sensibles ou non. Il ne serait pas non plus acceptable de limiter ces garanties aux cas dans lesquels le but de la surveillance est de collecter des données sensibles — ce qui semble plutôt rare - ; dans l'hypothèse d'une telle limitation, aucune garantie ne s'appliquerait aux cas, plus fréquents, dans lesquels il arrive que des systèmes de surveillance enregistrent occasionnellement, incidemment ou périodiquement des données sensibles.

On pourrait donc envisager d'élaborer, en se référant (expressément ou pas) au paragraphe 3 de la Recommandation n° R(89)2, quelques lignes directrices dont la teneur devrait, au moins :

- suggérer d'éviter de filmer des lieux réservés aux employés à des fins autres que le travail (toilettes, douches, vestiaires, zones de repos),

- inviter à consulter les employés pour l'installation de systèmes et d'équipements lorsqu'elle répond à des impératifs d'organisation, de production ou de sécurité du travail, en précisant la finalité de cette installation, le fonctionnement du système, ses capacités et l'utilisation qui doit en être faite, ainsi que l'heure et les circonstances des enregistrements ;

- accorder aux employés le droit de fonder, eux aussi, leurs contestations sur des séquences des enregistrements qui ont servi, en tout ou en partie, à motiver les plaintes portées à leur encontre.

12) PRINCIPES A INCLURE OU À PRÉCISER

Il conviendrait d'insister sur les principes de sélectivité et de proportionnalité dans tout nouvel instrument que le Conseil de l'Europe pourrait décider de consacrer à la surveillance ou à la vidéo-surveillance, en indiquant que les systèmes de surveillance ne devraient être mis en place que lorsqu'ils répondent à une réelle nécessité et visent à prévenir ou dépister des actes criminels ou à protéger les droits de tiers et lorsque le recours à une méthode de collecte de données empiétant moins largement sur la vie privée n'est pas possible.

Si le principe de la proportionnalité n'est pas respecté, on risque fort d'assister, au cours des prochaines années, à une augmentation exponentielle du nombre de lieux publics et privés placés sous surveillance et l'on aboutirait alors à une société imposant des restrictions excessives à la liberté personnelle. Toujours pour ce qui est de la proportionnalité, il ne faudrait pas se contenter d'énoncer le principe selon lequel la surveillance doit reposer sur des finalités licites, prévus par des dispositions législatives ou autres, à caractère souvent général (Footnote 20); en effet, ces dispositions risquent d'être interprétées de manière à justifier la mise en place d'une surveillance pour

prévenir non seulement les infractions pénales, mais aussi les contraventions à des dispositions du droit administratif ou civil ou à des règlements disciplinaires. Par exemple, une surveillance ne devrait pas être mise en place pour détecter les violations de l'interdiction de fumer dans des toilettes publiques (Footnote 21) ou de jeter des déchets ou des mégots de cigarettes sur la voie publique (Footnote 22).

En d'autres termes, la surveillance doit se limiter à des zones où les risques sont réels (Footnote 23), ainsi qu'aux manifestations lors desquelles on peut raisonnablement redouter des incidents ou des infractions plus graves.

Le principe de la pertinence des données collectées pour les finalités recherchées et la pondération avec laquelle elles doivent être exploitées doit être affirmé plus clairement par le Conseil de l'Europe. En particulier, s'agissant de la vidéosurveillance, il faudrait appeler les opérateurs concernés à :

- définir précisément, et dans tous les cas, la localisation des caméras et les modalités d'enregistrement (stockage et conservation des images, angles de prise de vue, restrictions éventuelles pour ce qui est des gros plans et du scannage des images) ;

- réduire le champ visuel en fonction du but recherché Footnote 24 ou des zones dans lesquelles une surveillance est effectivement nécessaire, en portant une attention particulière aux cas dans lesquels des caméras filmant des lieux publics permettent d'enregistrer des sons et des images provenant de lieux privés situés à proximité ;

- filmer, par principe et en fonction des contraintes techniques, d'une manière qui ne permette d'obtenir qu'une vue panoramique de la zone sous surveillance, sans possibilité de réaliser des gros plans et des agrandissements ultérieurs et en évitant les détails ou les caractéristiques physiques ne présentant aucun intérêt pour les buts recherchés.

13) INFORMATION DE LA PERSONNE CONCERNEE

L'on peut admettre que les informations communiquées aux personnes concernées n'indiquent pas la localisation des dispositifs de surveillance. Toutefois :

- ces dispositifs doivent au préalable être précisément énumérés par le responsable du traitement des données de surveillance et recensés dans le document de déclaration ou d'enregistrement susmentionné, qui sera déposé auprès d'une autorité publique (de préférence indépendante) ;

- les informations ne doivent pas être communiquées au moyen d'un panneau éloigné (situé par exemple à une distance pouvant aller jusqu'à 500 mètres, comme c'est déjà parfois le cas), mais d'un panneau situé à une distance raisonnable ;

- concernant les symboles visuels, l'on peut mentionner très brièvement la possibilité (déjà testée) de donner deux différents types d'informations en utilisant soit le symbole de la caméra si les images ne sont pas enregistrées, soit un autre symbole si les images sont également enregistrées ;

- l’obligation d’informer clairement les personnes concernées (cette information pouvant être sommaire, à condition d’être efficace) devrait être énoncée plus précisément, même dans des cas sans rapport avec l’usage de réseaux électroniques ;

- toutes les restrictions qui entourent l’information des personnes concernées devraient être réellement proportionnées au but poursuivi. Il pourrait être opportun de préciser (comme c’est le cas dans quelques systèmes juridiques, comme le système italien) que lorsque les données sont recueillies à des fins d’investigation ou de contestation d’un droit en justice, ces restrictions sont temporaires et ne s’appliquent que tant que la communication d’informations peut raisonnablement passer pour préjudiciable à la réalisation des buts précités.

En outre, si l’on décide d’inclure un paragraphe sur le consentement, il serait peut-être judicieux de préciser qu’au moins dans certaines circonstances, le consentement de la personne concernée peut également s’exprimer par son comportement probant – à condition que celle-ci ait reçu des informations claires.

14) COMMUNICATION

Il serait nécessaire de poser le principe de l’interdiction de la diffusion d’images et de leur communication à des tiers qui ne sont pas concernées par les activités de surveillance ; en outre, il conviendrait de préciser dans quels cas, selon quelles modalités et à quelles fins cette communication est autorisée.

15) INTERCONNEXION

Le principe de proportionnalité pourrait être davantage détaillé à cet égard afin d’identifier les cas dans lesquels l’indexation des données de surveillance est autorisée. Cette indexation – particulièrement lorsqu’elle est nominative – ne devrait être autorisée que par des dispositions spécifiques conformes au principe de proportionnalité.

De plus, ce principe devrait être défini avec plus de précision afin de limiter l’appariement des données de surveillance traitées par différents responsables du traitement aux cas dans lesquels cet appariement est réellement nécessaire aux fins prévues par la loi – en particulier s’il vise à suivre la « trajectoire » d’une personne en particulier.

16) DROIT D’ACCES

Les droits des personnes concernées devraient être pris en compte dans leur intégralité, comme c’est le cas dans la législation communautaire ; il ne faudrait pas se contenter de faire référence aux droits d’accès et de rectification.

Compte tenu des considérations précédentes, il serait envisageable de traiter aussi les questions suivantes :

- une personne concernée qui ne peut s’opposer à la surveillance devrait bénéficier du droit de s'opposer, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à certains types de traitement des données, comme le prévoit l’article 14

de la directive 95/46/CE. Ce principe devrait au moins s'appliquer à certains des cas dans lesquels la surveillance est autorisée par la loi même sans le consentement de l'intéressé, ainsi qu'aux cas dans lesquels la personne concernée, informée qu'une surveillance licite est exercée, ne peut en pratique que donner son consentement, par son comportement probant (lorsque, par exemple, elle se trouve sur une voie publique ou dans une banque où la surveillance est signalée). L'on pourrait citer un cas survenu en Italie, dans lequel une employée qui avait accepté la surveillance systématique de ses activités sur son lieu de travail afin d'illustrer, dans un but documentaire, certaines phases de production (dans le domaine du tannage du cuir) s'était toutefois opposée à la diffusion de ces images à des fins publicitaires.

Par ailleurs, la nécessité de concilier dans une certaine mesure le droit d'accès et la nature spécifique des données traitées est tout à fait compréhensible, compte tenu également des supports d'enregistrement utilisés. Il semble toutefois inacceptable que cette nécessité conduise à exclure le droit d'accès lorsque la personne concernée n'est pas identifiée mais identifiable.

De fait, s'il est jugé nécessaire de restreindre le droit d'accès, il faudra tenir compte du fait que l'article 9 (2) litt. b) de la Convention n° 108 du Conseil de l'Europe n'autorise de telles restrictions que dans certaines conditions, c'est-à-dire lorsqu'elles sont nécessaires pour protéger les droits et libertés d'autrui.

Par exemple, on pourrait préciser que la personne concernée peut toujours demander l'accès aux données, dans la mesure où cette demande est l'expression d'un droit véritable, et non pas d'un simple « intérêt légitime » ; toutefois, dans certaines circonstances le responsable du traitement des données de surveillance peut légalement s'abstenir de répondre à la demande et/ou de traiter les données de telle sorte que la personne concernée soit identifiable si ce procédé exige un effort manifestement disproportionné – sans préjudice des mesures et dispositions que pourraient prendre les forces de l'ordre ou les autorités judiciaires conformément à la loi.

Il convient en outre d'examiner s'il serait opportun d'interdire la récupération et la communication des données lorsque celles-ci doivent être détruites dans un délai très court (2 ou 3 jours ou une semaine, par exemple) ; cela n'exclurait nullement la possibilité d'accéder à ces données pour la défense d'un droit en justice ou en vue de produire des éléments de preuve pour se conformer à une décision des autorités de police ou des autorités judiciaires.

Il ne devrait être possible de priver la personne concernée de son droit d'accès pour protéger l'intérêt légitime d'un tiers que si le responsable du traitement des données ne peut prendre des mesures techniques visant à concilier les droits de la personne concernée et ceux du tiers faisant aussi l'objet du traitement. C'est ce qui se produit, par exemple, en cas d'agrandissement partiel ou de brouillage d'images montrant plusieurs personnes. L'accès aux données devrait systématiquement être autorisé s'il est nécessaire à la défense d'un droit en justice.

On pourrait prévoir expressément les cas dans lesquels l'accès peut être ajourné légalement (à titre temporaire toutefois) aussi longtemps que la divulgation des données par le responsable du traitement compromettrait réellement le droit de ce dernier à la défense d'un droit en justice. L'on pourrait à cet égard renvoyer aux

preuves recueillies dans les cas d'infidélité conjugale ou autre, que l'avocat de la défense pourrait prévoir de produire au procès à la suite des investigations menées par un détective privé dans le respect de la législation interne.

Enfin, il serait souhaitable de mentionner de façon spécifique les cas dans lesquels l'autorisation d'accès permet uniquement l'examen des données, celles-ci ne pouvant être enregistrées sur aucun support.

17) CONSERVATION DES DONNEES

S'agissant de la durée et des modalités de conservation des données, il devrait incomber au responsable du traitement des données de surveillance d'apprécier – avant même de décider de la durée pendant laquelle les données doivent être conservées en rapport avec les buts à atteindre – le responsable du traitement des données de surveillance doit apprécier s'il est nécessaire, à la lumière des objectifs poursuivis, de conserver les données ou s'il suffit que celles-ci puissent être visualisées (ex. système de télévision en circuit fermé utilisé pour contrôler l'ouverture des portes et des entrées) Footnote 25.

Par ailleurs, les délais fixés pour chaque type d'activité de surveillance ne devraient nullement exclure la possibilité ni l'obligation pour le responsable du traitement des données de surveillance ou un tiers de conserver plus longtemps les données éventuellement extraites en vue de la constatation ou de la défense d'un droit en justice. Il pourrait par ailleurs être suggéré que les responsables du traitement des données de surveillance ne puissent pas effacer ni détruire les données si une demande de conservation desdites données est soumise par la personne concernée ou un tiers en vue de la constatation ou de la défense d'un droit en justice.

18) RESPECT DES PRINCIPES

Il convient de réaffirmer le principe selon lequel le traitement des données à caractère personnel à des fins de surveillance doit être soumis au contrôle d'une autorité indépendante – conformément au principe 1.1 de la Recommandation n° R (87) 15.

Cela est particulièrement important pour ce qui concerne les autorités locales (communes, provinces, régions) : bien qu'elles ne soient pas, en principe, directement compétentes en matière d'ordre public – ce qui pourrait conduire à considérer qu'elles se situent en dehors du champ d'application de la Recommandation n° R (87) 15 -, ces autorités exercent en fait diverses activités accessoires à des fins de surveillance.

Hormis cette mention générale et solennelle, il conviendrait d'examiner si l'on pourrait préciser que les systèmes de surveillance devraient au moins faire l'objet d'une simple déclaration ou d'un enregistrement auprès d'une autorité de police ou d'une autorité indépendante – afin de garantir la transparence et de promouvoir la protection des droits des personnes concernées tout en assurant le contrôle de l'autorité susmentionnée (Footnote 26). L'on pourrait en outre suggérer que soient précisés, pour certains systèmes de surveillance impliquant une intrusion plus profonde dans la vie privée, les cas dans lesquels un contrôle préalable (conformément aux dispositions pertinentes de l'article 20 de la Directive 95/46/CE) ou l'approbation préalable d'une autorité seraient requis.

Si les activités de surveillance effectuées par les médias sont aussi prises en considération (ce qui semble souhaitable), les mécanismes envisagés pour porter à la connaissance du public les opérations de traitement devraient être mis en conformité avec la Recommandation n° R (94) 13 du 22 novembre 1994 sur des mesures visant à promouvoir la transparence des médias.

En conclusion, le Conseil de l'Europe est confronté à l'alternative suivante : élaborer une nouvelle recommandation sur la surveillance ou définir des principes directeurs à inclure dans un autre type d'instrument.

Les deux solutions sont dignes d'intérêt. Vingt ans après l'adoption de la Convention n° 108 du Conseil de l'Europe, ce qui importe réellement, c'est que l'Organisation fasse une fois encore entendre et respecter sa voix.

Footnotes

1) Dans la recommandation 99/1 adoptée les 9-10 juin 1999 par le « Standing Committee of the European Convention on Spectator Violence and Misbehaviuor at Sport Events and in particular at Football Matches » l'on attire l'attention sur l'observation des toutes les zones de danger potentiel et sur la prévention de l'excès de foule, mais aussi (bien que de manière générique) sur l'information du public sur tous les dispositifs de sécurité installés par les organisateurs.

2) Il suffit de penser au système DcxNet, qui – dit-on – peut faciliter la conduite lorsqu'il est associé à des systèmes de radar en agissant sur le frein, le volant, etc., et même en guidant le conducteur par mauvais temps (brouillard, par exemple). C'est un exemple d'application de réseaux électroniques à la circulation routière.

3) Dans la recommandation n° R(96) 6 du Comité des ministres sur la protection de l'Héritage culturel contre les agissements illicites – adoptée le 19 juin 1996 – au point 4 l'on affirme que, parmi les mesures préventives relatives aux musés, cathédrales etc., le plan de prévention devrait inclure des mesures de surveillance électronique (détection, centre de contrôle, transmission, télévision à circuit fermé, monitorage des accès, vidéosurveillance etc.).

4) A titre d'exemple, v. l'annonce faite le 11 septembre 2000 par la Visionics Corporation (http://www.visionics.com) concernant la nouvelle version de son système « FaceIt Sentinel/Surveillance 2.0 ».

5) Ainsi, lors de l'annonce du lancement du système « Echelon2 », le système « Echelon1 » n'avait pas encore été entièrement dévoilé.

6) Récemment, lors d'une réunion avec le ministre de la Justice italien, 220 aumôniers italiens ont déclaré que les détenus ne venaient malheureusement plus se confesser car ils craignaient que des micros ne fussent cachés dans les confessionnaux.

7) Les risques qu'une utilisation massive de la vidéo-surveillance posent pour le droit à l'autodétermination informative et à la libre circulation dans les espaces publics ont été mis en lumière dans la résolution adoptée par la 59ème Conférence des autorités allemandes pour la protection des données, qui s'est déroulée à Hanovre les 14 et 15 mars 2000 (« risques et limites de la vidéo-surveillance »).

8) Mme Marie-Odile Wiederkehr, Discours d'ouverture, Data Protection in the Police Sector, Conseil de l'Europe, Strasbourg, 13 décembre 1999, p. 10.

9) A. PATJIN, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13 December 1999, page 17.

10) Rapport explicatif sur la Convention, paragraphe 46.

11) A. PATJIN, Data Protection in the Police Sector, Conseil de l'Europe, Strasbourg, 13 décembre 1999, p. 18.

12) En particulier, le Comité Consultatif a été de l'avis que le traitement digital de voix et image constitue en tout cas une « élaboration automatisée », alors que le traitement analogique peut être ainsi qualifié seulement lorsque les voix et images sont élaborées en forme automatisée pour identifier les personnes concernées ou pour contribuer à leur identification.

13) Ainsi, en définissant les conditions de licéité s'appliquant à la (vidéo-) surveillance, il ne faudrait pas affaiblir les garanties prévues par la recommandation n° R(87)15 ; cette dernière exige en effet que :

- la collecte de données soit effectuée pour la prévention d'un danger *concret* (2.1) ;
- la surveillance soit prévue par des dispositions *spécifiques* (2.3) ;
- l'on évite la collecte de données concernant des personnes en raison de leur seule appartenance raciale etc. (2.4).

14) La définition couvrirait ainsi et le monitorage des communications en réseau, et la surveillance satellitaire, et les opérations de surveillance visant à la localisation de personnes (par exemple, via les impulsions des téléphones mobiles).

15) Il convient de mentionner à cet égard deux arrêts de la Cour de cassation italienne, à savoir les arrêts n° 7063/2000 et 8250/2000.

16) C'est par exemple le cas d'images transmises à la police montrant un revendeur de drogue, filmé par hasard, à proximité des toilettes d'un magasin, par un dispositif de surveillance installé par le propriétaire de ce magasin en violation de la loi.

17) Une indication similaire (bien que répondant à une autre finalité, puisqu'elle vise à permettre l'interception légale des télécommunications) figure aux points II, 5 et VI, 15 de la Recommandation n° R(95)13 relative aux problèmes de procédure pénale liés à la technologie de l'information.

18) Voir aussi la Recommandation n° R(95)4 du Conseil de l'Europe sur les télécommunications préconisant l'anonymat de l'accès aux réseaux et services de télécommunication (point 2.2).

19) Dans sa décision relative à la légalité du traitement de données erronées par les Services de renseignements roumains (SRI), la Cour a considéré :

« [qu'en ce qui concerne] l'exigence de prévisibilité, [...] aucune disposition du droit interne ne fixe les limites à respecter dans l'exercice de ces prérogatives. Ainsi, la loi interne ne définit ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre. De même, la loi ne fixe pas de limites quant à l'ancienneté des informations détenues et la durée de leur conservation. Quant à l'article 45, celui-ci habilite le SRI à reprendre, à toutes fins de conservation et utilisation, les archives ayant appartenu aux anciens organes de renseignements compétents sur le territoire de la Roumanie, et autorise la consultation des documents du SRI sur approbation du directeur. La Cour relève que cet article ne renferme aucune disposition explicite et détaillée sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues.

Elle note aussi que, bien que l'article 2 de la loi habilite les autorités compétentes à autoriser les ingérences nécessaires afin de prévenir et contrecarrer les menaces pour la sécurité nationale, le motif de telles ingérences n'est pas défini avec suffisamment de précision.

[En outre,] la Cour relève que le système roumain de collecte et d'archivage d'informations ne fournit [aucune] garantie[s], aucune procédure de contrôle n'étant prévue par la loi n° 14/1992, que ce soit pendant que la mesure ordonnée est en vigueur ou après.

Dès lors, la Cour estime que le droit interne n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. La Cour en conclut que la détention et l'utilisation par le SRI d'informations sur la vie privée du requérant n'étaient pas « prévues par la loi », ce qui suffit à constituer une méconnaissance de l'article 8. Au surplus, en l'espèce, cette circonstance empêche la Cour de contrôler la légitimité du but recherché par les mesures ordonnées, et si celles-ci étaient, à supposer le but légitime, « nécessaires dans une société démocratique ».

20) La mise en place, par les collectivités locales, de systèmes de surveillance globale visant à la fois la prévention des délits relevant de leurs compétences (infractions au code de la route, accès au centre ville) et une amélioration de la prévention et du contrôle de la criminalité (bien que ces collectivités n'aient pas forcément des compétences directes en matière d'ordre public) soulève un problème particulier.

21) Ce qui s'est passé en Belgique, dans un lycée technique.

22) Selon certaines informations, un système de surveillance aurait même été installé, à l'insu des personnes concernées, aux guichets d'un service public d'une ville allemande.

23) C'est par exemple l'approche retenue par les autorités françaises, qui citaient, dans une circulaire du 22.10.96, les lieux isolés et les commerces ouverts jusqu'à une heure tardive.

24) En Italie, l'autorité de protection des données à caractère personnel a exigé que le champ des caméras utilisées pour repérer les infractions au code de la route soit limité à la zone où se trouve normalement la plaque d'immatriculation. Cette restriction est importante, par exemple pour protéger la vie privée du conducteur.

25) A titre d'exemple, un règlement récemment adopté en Italie (n° 250/1999) prévoit que les systèmes de surveillance des accès aux centres urbains et aux zones piétonnes ne recueillent des images que si des infractions sont commises.

26) Les Parties pourraient par exemple reprendre une partie du formulaire de notification couramment utilisé pour la notification de nombreuses opérations de traitement des données.

Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données à caractère personnel au moyen de la vidéo-surveillance

AVANT-PROPOS

De nombreux organismes publics et privés ont de plus en plus recours, à des fins diverses et dans différents secteurs, à des systèmes de surveillance qui leur permettent de contrôler en particulier la circulation des personnes et des biens et l'accès aux propriétés, mais aussi certaines manifestations, situations ou conversations, par le biais de réseaux téléphoniques ou électroniques, ou de systèmes installés sur place.

Les systèmes de surveillance conduisent souvent à recueillir des données à caractère personnel dont la collecte et/ou l'enregistrement n'est parfois pas le but recherché par le responsable du traitement des données de la surveillance.

Une très grande partie de ces activités fait appel à des dispositifs de vidéo-surveillance qui posent des problèmes particuliers de protection des données.

En effet, les données collectées à l'occasion d'activités de vidéo-surveillance se composent essentiellement d'images et de sons qui permettent d'identifier les personnes concernées, directement ou non, tout en surveillant leur comportement.

Les activités de vidéo-surveillance impliquant le traitement de données à caractère personnel entrent dans le champ d'application de la Convention n° 108 du Conseil de l'Europe, dont les principes reposent sur les dispositions contenues dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Des droits et garanties complémentaires sont énoncés dans diverses recommandations du Conseil de l'Europe et, en particulier:

a. la Recommandation n° R(87)15 sur l'utilisation des données à caractère personnel dans le secteur de la police;

b. la Recommandation n° R(89)2 sur la protection des données à caractère personnel utilisées à des fins d'emploi;

c. la Recommandation n° R(95)4 sur la protection des données à caractère personnel dans le secteur des télécommunications;

d. diverses autres recommandations qui, si elles ne renvoient pas expressément à la vidéo-surveillance, contiennent des garanties et des règles qui sont pertinentes pour la protection des données à caractère personnel ainsi que pour la communication des données et leurs échanges transfrontaliers.

La vidéo-surveillance pose des problèmes spécifiques de protection qui ne sont pas examinés en détail dans les instruments évoqués; cette situation s'explique en partie

par les mécanismes de collecte et d'enregistrement des données, mais aussi par l'évolution technologique.

Il est donc nécessaire de fixer quelques principes directeurs afin d'étendre et de préciser les garanties qui s'appliquent – sans préjuger de la protection déjà accordée par les instruments ci-dessus dans leurs secteurs respectifs - aux personnes concernées par tout type d'activité de vidéo-surveillance qui, par le recours à des instruments techniques, observe, collecte et/ou enregistre de manière non occasionnelle des données à caractère personnel concernant les comportements, mouvements, communications ou utilisations de réseaux informatiques ou électroniques d'une ou plusieurs personnes.

Ces principes directeurs sont destinés à être diffusés auprès du public et auprès des usagers privés de systèmes de vidéo-surveillance et autres moyens et dispositifs de surveillance; en outre, ils s'adressent aux Etats membres, aux fabricants, aux revendeurs, aux fournisseurs de services et d'accès et aux chercheurs afin que des logiciels et des technologies puissent être développés qui accordent une plus grande part aux droits fondamentaux des personnes concernées par la vidéo-surveillance.

Ces principes directeurs devraient aussi s'appliquer à d'autres activités de surveillance qui ne reposent pas sur l'utilisation d'appareils de vidéo-surveillance, sous réserve d'adaptations en conséquence.

PRINCIPES DIRECTEURS POUR LA PROTECTION DES PERSONNES PAR RAPPORT À LA COLLECTE ET AU TRAITEMENT DE DONNÉES A CARACTERE PERSONNEL AU MOYEN DE LA VIDÉO-SURVEILLANCE

Toute activité de vidéo-surveillance suppose:

1. de vérifier si et dans quelle mesure elle est autorisée sur des bases juridiques appropriées à des fins légitimes, spécifiques, et explicites, et si elle est menée de manière loyale. Les activités de vidéo-surveillance à des fins de police ne devraient être entreprises que pour prévenir un danger concret ou pour réprimer une infraction déterminée;

2. de prendre les mesures nécessaires pour veiller à ce que cette activité soit conforme aux principes en matière de protection des données à caractère personnel.

3. de n'utiliser des appareils de vidéo-surveillance que si l'on ne peut appliquer d'autres systèmes portant moins atteinte à la vie privée;

4. de respecter les principes de sélectivité et de proportionnalité concernant les objectifs recherchés dans les cas individuels afin d'empêcher toute atteinte inconsidérée aux libertés et aux comportements des personnes concernées (le cas échéant, ces libertés peuvent comprendre le consentement de la personne concernée, qui pourrait être exprimé au moins, de manière probante) – notamment à la liberté de circulation et au droit à l'autodétermination en matière d'information – et en veillant à respecter raisonnablement la vie privée, même dans des lieux publics;

5. de respecter le principe selon lequel les données doivent être pertinentes et non excessives – du point de vue des données visuelles, sonores et biométriques collectées –, notamment au regard des moyens techniques utilisés (par exemple caméras fixes ou mobiles, étendue du champ visuel, possibilité d'agrandir les images, etc.) et en empêchant que les informations collectées ne puissent être conservées, indexées ou gardées longtemps si cela n'est pas nécessaire pour le but spécifique recherché;

6. de limiter les activités de vidéo-surveillance si elles peuvent conduire à des formes de discrimination ou si elles ont été ordonnées pour certaines personnes exclusivement au regard de leurs opinions, de leurs convictions ou de leur vie sexuelle;

7. de respecter le principe de transparence, c'est-à-dire d'informer de l'existence d'une activité spécifique de vidéo-surveillance (en prévoyant un système de notification – accessible au public – à un organisme public de préférence indépendant) et en informant les personnes concernées (en fournissant des informations claires, même sommaires, accompagnées de panneaux signalant de façon visible la localisation des appareils de surveillance). Les restrictions à la transparence et aux exigences d'information ne devraient être autorisées que dans des limites raisonnables et proportionnées, et quand elles sont nécessaires pour protéger les droits, les libertés et les objectifs évoqués à l'article 9 de la Convention n° 108;

8. de veiller à renforcer la protection en cas de dangers spécifiques pour les personnes concernées et/ou de contrôles plus envahissants concernant par exemple:

- l'association d'images et de données biométriques;

- l'utilisation de systèmes d'analyse intelligente et d'intervention;

- des logiciels pour la consultation automatique d'images ou pour la reconnaissance des visages;

- l'indexation des données collectées;

- la définition de profils pour les personnes concernées;

- la possibilité de prendre des décisions automatisées par rapport aux compétences professionnelles, à la productivité, à la fiabilité, à l'origine ethnique;

- la vidéo-surveillance visant à contraindre les citoyens à se comporter conformément à un schéma donné.

9. La communication de données à caractère personnel à des tiers qui ne sont pas concernés par l'activité de surveillance doit être interdite en principe, sous réserve de préciser les cas dans lesquels elle peut être autorisée dans le cadre de dispositions pertinentes et pour des finalités spécifiques;

10. de définir des dispositions ad hoc pour l'exercice du droit d'accès et autres droits des personnes concernées, et de ne prévoir des restrictions à ces droits que dans une mesure raisonnable et proportionnée lorsque cela s'avère nécessaire pour la protection

des droits, libertés et objectifs définis à l'article 9 de la Convention n° 108. En particulier, l'exercice du droit d'accès doit aussi être autorisé (même sous forme d'un visionnage des images) si la personne concernée peut être identifiée. Les responsables du traitement des données de surveillance doivent être autorisés à refuser l'accès si cela suppose un travail visiblement disproportionné ou si les données vont être détruites à brève échéance – sous réserve de protection des droits de la défense en cas d'action en justice;

11. de limiter l'utilisation des systèmes visant à la surveillance délibérée de la qualité du travail et de la productivité sur le lieu de travail et de veiller à ce que les employés soient convenablement informés – si nécessaire en accord avec les syndicats concernés si de tels systèmes doivent être mis en place en raison d'exigences organisationnelles ou de production, ou à des fins de sécurité au travail nécessitant une surveillance à distance; il convient de respecter dans tous les cas la dignité humaine des employés, y compris la possibilité d'établir des liens sociaux et personnels sur le lieu de travail. Dans ce contexte, les employés devraient pouvoir s'appuyer sur les enregistrements effectués en cas de litige ou de revendication.