Groupe de travail "Article 29" sur la protection des données

**11750/02/FR**
**WP 89**

# Avis
# 4/2004 sur le traitement des données à caractère personnel au moyen de la vidéo-surveillance

**Adopté le 11 février 2004**

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE.

Le secrétariat est assuré par la Commission européenne, DG Marché intérieur, Direction E "Services, Droit d'auteur, Propriété Industrielle et Protection des Données", B-1049 Bruxelles - Belgique - Bureau: C100-6/136

Adresse Internet: www.europa.eu.int/comm/privacy

**LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES À CARACTERE PERSONNEL**

Établi par la directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995[1],

vu l'article29 et l'article30, paragraphes 1 (a) et 3 de ladite directive,

vu son règlement intérieur, notamment les articles12 et 14,

A ADOPTÉ LE PRÉSENT AVIS:

## 1. Introduction

Depuis quelques années, des organismes publics et privés en Europe ont de plus en plus recours à des systèmes d'acquisition d'images. Ce phénomène a suscité des discussions animées, tant au niveau communautaire que dans les États membres, afin de déterminer les conditions et les limites applicables à l'installation des équipements permettant d'effectuer une vidéo-surveillance, ainsi que les garanties nécessaires pour les personnes concernées.

L'expérience de ces dernières années, qui suit également la transposition dans les États membres de la directive n° 95/46/CE, a mis en évidence une prolifération énorme d'installations à circuit fermé, de caméras et d'autres moyens plus sophistiqués utilisés dans les secteurs les plus différents.

L'évolution des technologies disponibles, la numérisation et la miniaturisation multiplient considérablement les opportunités fournies par les moyens d'enregistrement visuel et sonore, et notamment leur utilisation sur les réseaux *intranet* et *Internet.*

En plus du contexte des lieux de travail publics et privés, qui a déjà été analysé par le groupe dans un document détaillé (*Avis 8/2001 sur le traitement de données personnels dans le milieu du travail*[2]*),* la prolifération croissante des techniques de vidéo-surveillance peut être facilement constatée par le public. La tendance est également au renforcement de l'interconnexion des systèmes de vidéo-surveillance.

Une analyse non exhaustive des applications principales montre que les finalités de la vidéo-surveillance sont très différentes[3], mais peuvent toutefois être regroupées en des catégories spécifiques:

---

[1] Journal Officiel n° L 281 du 23/11/1995, p. 31, disponible au site :
*http://europa.eu.int/comm/internal_market/fr/dataprot/index.htm*

[2] WP 48, adopté le 13 septembre 2001, disponible au site:
*http://europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm*

[3] Différents systèmes de vidéo-surveillance sont installés:

a) à l'intérieur et à proximité d'établissements publics et/ou de bâtiments ouverts au public, afin de prévenir des actes illicites ou des faits moins graves de vandalisme ;
b) à l'intérieur des stades et d'installations de sport, en particulier à l'occasion d'événements particuliers;
c) dans le secteur des transports et en relation avec la circulation routière, afin de surveiller la circulation sur les autoroutes et les routes à grande circulation, ou bien pour détecter les infractions aux limites de vitesse ou à des dispositions concernant la circulation des véhicules dans le centre ville, ou encore afin de contrôler les voies souterraines d'accès au métro, les stations à essence, ainsi qu'à l'intérieur des taxis ;
d) afin de prévenir ou de vérifier des comportements illicites à proximité des écoles, notamment en relation avec le racolage de mineurs ;
e) à l'intérieur d'établissements de santé, pendant des opérations chirurgicales, ou afin, par exemple, d'assister ou contrôler à distance des patients en soins intensifs, ou en des secteurs réservés à des malades graves ou en isolément ;

1) protection des personnes;
2) protection des biens;
3) intérêt public;
4) détection, prévention et répression d'actes illicites;
5) acquisition d'éléments de preuve;
6) d'autres intérêts licites.

Les conditions permettant l'installation de vidéo-caméras et d'autres appareils similaires sont également différentes.

Dans certains cas, l'emploi d'un système d'enregistrement visuel peut être rendu obligatoire par des dispositions spécifiques des États membres (par exemple, dans certains casinos); en d'autres cas, il répond à une finalité particulièrement importante pour les membres de la famille des personnes concernées (recherche de personnes ou de mineurs disparus). On peut citer également des cas sortant de l'ordinaire – surtout dans des pays tiers – où des systèmes de reconnaissance automatique du visage ont été mis au point afin d'empêcher de faux mariages; parfois, une autorité de police locale a décidé de diffuser publiquement et en continu des images de la dure condition de vie des prisonniers, sans leur consentement.

Si dans certains cas la vidéo-surveillance peut se justifier, dans d'autres, on assiste à un recours impulsif à des techniques de protection par cameras, sans pour autant accompagner ce phénomène d'une réflexion adéquate sur les conditions et les modalités d'utilisation. Parfois, la cause doit être recherchée dans les avantages économiques accordés sur une grande échelle par des organismes publics ou bien dans les tarifs d'assurance avantageux dûs à l'utilisation de systèmes de vidéo-surveillance.
Un effet psychologiques est également associé à la vidéo-surveillance en ce sens qu'elle est parfois considérée par l'opinion publique, à tort ou à raison, comme un « instrument précieux » en raison du fait qu'elle a déjà permis la détection de délits.

Il s'agit donc d'un secteur complexe et qui ne cesse d'évoluer, dans lequel différentes techniques sont déjà disponibles.

Le présent document de travail fournit dons une première analyse qui a comme point de départ la partielle diversité des réglementations en la matière, ainsi que l'existence de dispositions ponctuelles dans les législations internes de chaque pays, ce qui exige une approche plus systématique et harmonisée.

Le document se réfère à la surveillance en vue du contrôle à distance d'événements, de situations et de faits spécifiques; il ne s'intéresse pas directement à d'autres cas concernant la publicité occasionnelle et/ou éventuelle d'événements en relation, par exemple, avec la transparence de l'activité d'organismes représentatifs parlementaires ou locaux.

---

f) à proximité des aéroports, à bord des navires et près des frontières, afin de surveiller l'immigration clandestine ou rechercher des personnes ou des mineurs disparus ;
g) par des détectives privés ;
h) à l'intérieur et à proximité des supermarchés et de commerces consacrés en particulier aux articles de luxe, aux fins de l'acquisition d'éléments de preuve en cas d'infraction, ainsi que pour la commercialisation de produits et l'analyse des comportements des consommateurs ;
i) à l'intérieur et à proximité de résidences, pour des finalités de sécurité personnelle et d'acquisition des éléments de preuve en cas d'infraction ;
j) pour des finalités de presse et de publicité poursuivies en ligne, au moyen de *web-cams* ou de *cameras en ligne* utilisées dans des buts de promotion touristique ou de publicité, installées sur certaines plages ou dans des boîtes de nuit, prévoyant, à des intervalles réguliers, des prises de vue sans avertissement des clients et des visiteurs.

Chaque opérateur pourra par la suite développer en détail les indications fournies en cette occasion, non seulement dans son secteur d'activité, mais aussi par rapport aux développements technologiques futurs que le groupe se réserve d'approfondir.

Les principes qui seront ci-après examinés sont en outre considérés en relation avec l'acquisition d'images, éventuellement associée à des sons et/ou à des données biométriques telles que les empreintes digitales[4].

Ces principes peuvent, lorsqu'ils sont concrètement applicables, être également pris en considération en ce qui concerne le traitement éventuel de données à caractère personnel effectué non au moyen d'appareils visuels, mais au moyen de formes différentes de surveillance, c'est à dire de contrôle à distance – c'est le cas, par exemple, des systèmes de localisation satellitaire Gps.

Ce document de travail vise en premier lieu à attirer l'attention sur le large éventail de critères d'évaluation du caractère licite et approprié de l'installation de systèmes de vidéo-surveillance.

Toutefois, les aspects qui suivent ont été également pris en considération :

a) la nécessité d'une évaluation à caractère générale de la vidéo-surveillance par les institutions concernées des États membres, afin d'encourager une approche globalement sélective et systématique en la matière. Il faut éviter qu'une excessive prolifération des systèmes d'acquisition d'images en des endroits publics et privés n'entraîne une restriction injustifiée des droits et libertés fondamentaux des citoyens; dans le cas contraire, les citoyens pourraient devoir se soumettre d'une manière disproportionnée à des procédures de collecte de données qui les rendraient massivement identifiables dans un grand nombre de lieux publics et privés;

b) l'utilité d'une évaluation des tendances de l'évolution des techniques de vidéo-surveillance, afin d'éviter que le développement d'applications logicielles basées sur la reconnaissance du visage des personnes et sur l'étude et la prévision des comportements humains enregistrés dans les images n'entraîne un passage massif et inconsidéré à une surveillance du type dynamique-préventive, par opposition à la forme la plus commune de surveillance statique, qui vise surtout à informer sur des événements spécifiques et leurs auteurs. Cette nouvelle forme de surveillance repose sur l'acquisition automatisée des traits du visage de personnes physiques et de leurs comportements "anormaux"; elle prévoit aussi la possibilité d'envoyer des signaux automatisés d'alarme et de demande d'intervention qui pourraient créer des risques de discrimination.

## 2 INSTRUMENTS JURIDIQUES INTERNATIONAUX

a) **Convention des Droits de l'homme et des libertés fondamentales**.

La protection de la vie privée est assurée par l'article 8 de la Convention des droits de l'homme.

**b) Convention du Conseil de l'Europe n° 108/1981 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel.**

[4] Le problème plus général de l'application de la directive 95/46/CE dans le domaine de la biométrie sera traité par le groupe de travail dans un document spécifique.

Le champ d'application de cette Convention ne se borne pas comme celui de la directive à des activités du premier pilier (voir ci-dessous). Les activités de vidéo-surveillance comportant le traitement de données à caractère personnel entrent dans le champ d'application de cette Convention. Selon le comité consultatif établi par cette Convention, les voix et les images doivent être considérées comme des données à caractère personnel lorsqu'elles fournissent des informations sur une personne en la rendant identifiable, même indirectement.

Le Conseil de l'Europe met la dernière main à un ensemble de principes directeurs pour la protection des personnes vis-à-vis de la collecte et du traitement de données au moyen de la vidéo-surveillance. Ces principes devront en outre spécifier en détail les mesures de protection applicables aux personnes concernées incluses dans les dispositions des instruments du Conseil de l'Europe.

### c) Charte des droits fondamentaux de l'Union européenne

La Charte des droits fondamentaux de l'Union européenne prévoit à l'article 7 la protection de la vie privée et familiale, de l'habitation et des communications et, à l'article 8, la protection des données à caractère personnel.

## 3. LA SURVEILLANCE AU SENS DE LA DIRECTIVE 95/46/EC

Le caractère spécifique du traitement de données à caractère personnel incluant des sons ou des images, a été souligné par la directive 95/46/EC (ci-après dénommée « la directive »), qui y fait expressément référence en plusieurs points.

Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel
(article 1, paragraphe 1).

Nombre d'informations récoltées au moyen des systèmes de vidéo-surveillance ont pour objet des personnes identifiées ou identifiables, qui ont été filmées en des lieux publics ou accessibles au public. En ces lieux, les personnes de passage s'attendent à un niveau de protection de la vie privée certainement plus réduit, sans toutefois envisager une privation totale de leurs droits et libertés en ce qui concerne également leur vie privée et leur image.

Une attention particulière doit être accordée au droit à la libre circulation des personnes qui se trouvent licitement sur le territoire de l'État; ce droit est sauvegardée par le protocole additionnel n° 4, article 2, de la Convention européenne des droits de l'homme et des libertés fondamentales.

La liberté de circulation ne peut être limitée que par des restrictions nécessaires dans une société démocratique et qui répondent à des finalités spécifiques. Les personnes concernées ont le droit d'exercer leur liberté de mouvement sans être soumises à un conditionnement psychologique excessif en ce qui concerne leurs mouvements et leurs comportements. Elles ne doivent non plus être soumises à un contrôle minutieux de leurs mouvements, tel que le suivi de leurs mouvements et/ou le déclenchement d' « alarmes » à partir de logiciels qui « interprètent » automatiquement le comportement apparemment suspect d'un individu, sans intervention humaine, en raison de l'utilisation disproportionnée de la vidéo-surveillance par différents organismes dans un certain nombre de lieux publics et/ou accessibles au public.

Le caractère spécifique et sensible du traitement de données relatives à des sons et images concernant des personnes physiques, est mis en évidence dans la directive dès les premiers considérants et par certains articles. Outre les considérations formulées ci-après en matière de champs d'application, les considérants et les articles correspondants précisent que:

a) la directive est en principe applicable en la matière en prenant également en considération l'évolution en cours des techniques qui permettent de capter, manipuler et utiliser d'une autre manière la catégorie spécifique de données à caractère personnel qui ont été ainsi collectées (considérant n° 14);
b) les principes de la directive en matière de protection sont applicables à toute information, y compris sous forme de sons et images, concernant une personne identifiée ou identifiable, en tenant compte de l'ensemble des moyens pouvant être raisonnablement utilisés par le responsable du traitement ou par d'autres personnes afin d'identifier ladite personne (article 2, a); considérant n° 26).

En plus des références spécifiques susmentionnées, la directive produit évidemment tout ses effets dans le cadre de ses dispositions spécifiques, concernant en particulier :

1) la *qualité des données*. Les images doivent être traitées de manière licite et loyale, ainsi que pour des finalités déterminées, explicites et légitimes. Les images doivent être utilisées conformément au principe selon lequel les données doivent être adéquates, pertinentes et non excessives; elles ne doivent pas être traitées ultérieurement d'une manière non compatible avec ces finalités; elles doivent être conservées pendant une période limitée, etc. (article 6);

2) Les *principes relatifs à la légitimation du traitement.* Ils exigent que le traitement de données à caractère personnel au moyen de la vidéo-surveillance soit nécessairement basé sur au moins l'une des conditions prévues à l'article 7 (consentement non ambigu, nécessité d'obligations contractuelles, respect d'une obligation de loi, sauvegarde d'un intérêt vital de la personne concernée, exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, équilibre des intérêts);

3) Le traitement de *catégories particulières de données*, qui est soumis aux garanties applicables en cas d'utilisation, dans le cadre de la vidéo-surveillance, de données sensibles ou concernant des infractions (article 8);
4) *L'information* des personnes concernées (articles 10 et 11);
5) Les *droits des personnes concernées,* en particulier le droit d'accès et celui de s'opposer au traitement pour des raisons prioritaires et licites (articles 12 et 14, a);
6) La garantie s'appliquant en cas de *décisions individuelles automatisées* (article 15);
7) La *sécurité* des traitements (article 17);
8) La *notification des traitements* (articles 18 et 19);
9) Le *contrôle préliminaire* des traitements qui présentent des risques spécifiques à l'égard des droits et libertés des personnes (article 20);
10) Le *transfert de données vers des Pays tiers* (article 25 et articles suivants).

Le caractère spécifique et délicat des traitements relatifs à des sons et images est mis en particulière évidence dans le dernier article de la directive, qui prévoit que la Commission effectue une analyse de l'application de la directive en la matière et qu'elle présente des propositions éventuellement nécessaires, compte tenu de l'évolution de la technologie de l'information et des progrès survenus dans la société de l'information (article 33).

## 4. Législation nationale applicable à la vidéo-surveillance

En différents États membres, il existe déjà des cas d'études en matière de vidéo-surveillance, qui reposent sur des normes constitutionnelles[5] ou sur des dispositions législatives spécifiques, des prescriptions ou d'autres décisions émanant des autorités nationales compétentes[6].

Dans certains pays, il existe également des dispositions spécifiques qui s'appliquent indépendamment du fait que la vidéo-surveillance comporte ou non le traitement de données à caractère personnel. Ces dispositions prévoient également que l'installation et la mise en œuvre d'un système CCTV (télévision a circuit fermé) et d'autres systèmes similaires de surveillance soient soumis à autorisation préalable de la part d'une autorité administrative, qui peut être représentée, en tout ou en partie, par l'autorité nationale pour la protection des données à caractère personnel. Les dispositions peuvent être différenciées sur la base de la nature publique ou privée de la personne responsable du fonctionnement de l'installation.

En d'autres pays, la vidéo-surveillance ne fait pas l'objet de dispositions de loi spécifiques; toutefois, les autorités de protection des données à caractère personnel ont opéré afin de garantir une application appropriée des dispositions générales de protection des données au moyen d'opinions, lignes directrices ou codes de conduite qui ont déjà été adoptés (Royaume Uni) ou qui sont en train d'être élaborés (Italie).

| | |
|---|---|
| Allemagne | Article 6 , point b de la loi fédérale 2000.<br>Article 25 de la loi sur la protection des frontières.<br>Autre réglementations en matière de vidéo-surveillance exercée par la police dans les législation des Länder sur la police.<br>Un projet de loi interdisant le recours à la vidéo-surveillance secrète est actuellement débattu par le parlement. |
| Belgique | Avis de l'Autorité chargée de la protection des données, en particulier avis d'initiative 34/99 du 13 décembre 1999, relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéo-surveillance; Avis d'initiative 3/2000 du 10 janvier 2000 relatif à l'utilisation de systèmes de vidéo-surveillance dans les halls d'immeubles à appartements |
| Danemark | Loi de synthèse n° 76 du 1er février 2002 relative à l'interdiction de la vidéo-surveillance. Cette loi interdit d'une façon générale aux entités privées d'exercer une vidéo-surveillance sur la voie publique et dans les squares ou toute zone équivalente de libre circulation.Il existe toutefois certaines dérogations à cette interdiction.<br>Décision de l'Autorité chargée de la protection des données du 3 juin 2002 concernant la vidéo-surveillance par un grand groupe de supermarchés et transmission directe sur Internet depuis un café. |

[5] Voir la Décision de la Cour constitutionnelle portugaise 255/2002. La Cour a statué que « l'utilisation de dispositifs électroniques de surveillance et le contrôle des citoyens par d'organismes de sécurité privés constituent une limitation ou une restriction du droit de protéger la vie privée, consacré par l'article 26 de la Constitution ».

[6] Dans un pays au moins (affaire Belgique-Gaia), la violation de la législation en matière de protection de données dans le cadre de la collecte d'images a conduit à un refus des éléments de preuve admissibles devant la Cour.

| | |
|---|---|
| | Décision de l'Autorité chargée de la protection des données du 1er juillet 2003 selon laquelle la vidéo-surveillance exercée par une société privée de transport public doit être adaptée et conforme aux dispositions de la loi sur la protection des données.<br><br>Décision de l'Autorité chargée de la protection des données du 13 novembre 2003 imposant certaines restrictions à la vidéo-surveillance exercée par les pouvoirs publics. |
| Espagne | Ley organica n° 4/1997 (vidéo-surveillance par les forces et les corps de sécurité en des lieux publics)<br><br>Real Decreto n° 596/1999 d'application de la l. n° 4/1997 |
| Finlande | En Finlande, il n'existe pas de législation spéciale en mati§re de vidéo-surveillance mais des dispositions d'un grand nombre de textes législatifs différents s'appliquent à la vidéo-surveillance ainsi qu'à d'autres systèmes de surveillance, d'observation et de contrôle techniques.<br><br>Des questions concernant la vidéo-surveillance et l'enregistrement des conversations sont fréquemment posées et un certain nombre de cas ont été enregistrés.<br><br>Ainsi, le médiateur pour la protection des données a rendu un avis sur l'enregistrement des conversations téléphoniques par les services de la clientèle et dans le milieu de travail (numéros de dossier 1061/45/2000 et 525/45/2000).<br><br>Notre bureau a publié une brochure sur la protection de la vie privée dans le cadre de la vidéo-surveillance (Asiaa tietosuojasta 4/2001 Yksityisyyden suoja kameravalvonnassa) http://www.tietosuoja.fi/uploads/03wamgvxuybt4ti.rtf. |
| France | Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (CNIL)<br><br>Recommandation de l'autorité chargée de la protection des données n° 94-056 du 21 juin 1994<br><br>Guide de l'autorité chargée de la protection des données concernant la vidéo-surveillance sur le lieu de travail: http://www.cnil.fr/thematic/index.htm; sur d'autres thèmes (par exemple les web-cam)[7]<br><br>Loi spécifique concernant la vidéo-surveillance aux fins de sécurité dans les lieux publics: loi n° 95-73 du 21 janvier 1995 relative à la sécurité (modifiée par l'ordonnance 2000-916 du 19 septembre 2000), décret n° 96-926 du 17 octobre 1996 et circulaire du 22 octobre |

[7] Cf. les rapports annuels de la Commission nationale française de l'informatique et des libertés.

| | |
|---|---|
| | 1996 sur la mise en œuvre de la loi n° 95-73. |
| Grèce | Lettre n°390 du 28 janvier 2000 concernant l'installation d'un système de télévision en circuit fermé dans le Métro d'Athènes.<br><br>Directive n°1122 du 26 septembre 2000 concernant la télévision en circuit fermé.<br><br>Décision n°84/2002 relative aux systèmes de télévision en circuit fermé dans les hôtels. |
| Irlande | Loi sur la protection des données de 1998 et de 2003<br><br>Étude de cas n° 14/1996 (utilisation de la CCTV) |
| Italie | Article 34 du code de protection des données à caractère personnel (D.lg. n°196 du 30 juin 2003 portant adoption du code de conduite)<br><br>Décisions de l'autorité de contrôle (Garante) n° 2 du 10 avril 2002 (promotion du code de conduite); 28 septembre 2001 (techniques biométriques et reconnaissance du visage près les banques) et 29 novembre 2000 (le "décalogue" sur la vidéo-surveillance)<br><br>d.P.R. 22 juin 1999, n° 250 (accès des véhicules aux centres historiques et aux zones à circulation limitée)<br><br>D.l. 14 novembre 1992, n° 433 et l. n. 4/1993 (musées, bibliothèques et archives de l'Etat)<br><br>D.lg. 4 février 2000, n° 45 (paquebots affectés à des voyages nationaux)<br><br>Article 4 l. 20 mai 1970, n° 300 (Statut des travailleurs) |
| Luxembourg | Articles 10 et 11 de la loi du 02.0802002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel |
| Pays-Bas | Le rapport de l'autorité chargée de la protection des données publié en 1997 contient des lignes directrices concernant la vidéo-surveillance, en relation notamment avec la protection des personnes et des biens dans les lieux publics. Une mise à jour des lignes directrices élaborées en 1997 sera disponible en 2004.<br><br>Enquête sur la vidéo-surveillance dans l'ensemble des municipalités néérlandaises en 2003.<br><br>Modification du code pénal entrant en vigueur à compter du 1er janvier 2004 et étendant le champ d'application de l'infraction consistant à photographier des lieux accessibles au public sans en informer les personnes.<br><br>Le gouvernement propose de modifier la loi sur les collectivités locales afin de donner explicitement |

| | |
|---|---|
| | compétence aux conseils municipaux et aux maires pour utiliser des systèmes de vidéo-surveillance dans le domaine public et pour des besoins publics sous certaines conditions (telles que l'obligation d'évaluer périodiquement l'efficacité de la vidéo-surveillance). |
| Portugal | Décret-loi 231/98 du 22 juillet 1998 (activités privées de sécurité et systèmes d'autoprotection)<br>Loi 38/98 du 4 août 1998 (mesures à adopter en cas de violence associée à des événements sportifs)<br>Décret-loi 263/01 du 28 septembre 2001 (discothèques)<br>Décret-loi 94/2002 du 12 avril 2002 (événements sportifs) |
| Royaume-Uni | CCTV Code of practice 2000 (Information Commissioner), en cours de révision. |
| Suède | La vidéo-surveillance est spécifiquement réglementée par la loi (1998:150) relative à la vidéo-surveillance générale et la loi (1995:1506) sur la vidéo-surveillance secrète (dans les enquêtes criminelles)[8].<br>La vidéo-surveillance générale requiert en principe l'autorisation d'une administration régionale bien qu'il y ait un certain nombre d'exceptions, par exemple, en ce qui concerne la surveillance des bureaux de poste, des banques et des magasins. La vidéo-surveillance secrète doit être autorisée par un tribunal. Le Chancellier de la justice peut faire appel d'une décision de la commission administrative régionale.<br>L'enregistrement vidéo par des caméras numériques est considéré comme un traitement de données à caractère personnel et est donc placé sous la supervision de l'autorité chargée de la protection des données dans la mesure où elle n'est pas spécifiquement réglementée par la loi relative à la vidéo-surveillance générale.<br>Une commission d'enquête a publié un rapport sur la vidéo-surveillance (SOU 2002 :110). |

[8] En Suède, La vidéo-surveillance générale requiert en principe l'autorisation d'une commission administrative régionale bien qu'il y ait un certain nombre d'exceptions, par exemple, en ce qui concerne la surveillance des bureaux de poste, des banques et des magasins. La vidéo-surveillance secrète doit être autorisée par un tribunal. Conformément à la loi relative à la vidéo-surveillance générale, le Chancellier de la justice peut faire appel d'une décision de la commission administrative régionale dans l'intérêt de la sécurité publique. L'enregistrement vidéo par des caméras numériques est considéré comme un traitement de données à caractère personnel en vertu de la loi sur la protection des données et est donc placé sous la supervision de l'autorité chargée de la protection des données. La commission d'enquête contrôle actuellement l'utilisation de la vidéo-surveillance pour la prévention des délits. La commission doit notamment évaluer la loi relative à la vidéo-surveillance générale pour déterminer si des modifications s'imposent. Elle vérifie également le champs d'application de la loi sur la protection des données en ce qui concerne la vidéo-surveillance et le besoin éventuel d'une législation particulière sur le traitement des données à caractère personnel en relation avec la vidéo-surveillance.

D'autres instruments qui méritent d'être mentionnées concernent l'Islande (article 4, loi n° 77/2000), la Norvège (titre VII loi n° 31 du 14 avril 2000), la Suisse (recommandation du Responsable fédéral) et la Hongrie (recommandation DPA du 20 décembre 2000) .

## 5. Secteurs auxquels la directive 95/46/EC est en tout ou en partie inapplicable

La directive n'est pas applicable au traitement de données sous forme de sons et images effectué pour des finalités concernant la sécurité publique, la défense, la sûreté de l'État ou l'exercice d'activités de l'État dans le domaine du droit pénal ou d'autres activités qui ne tombent pas dans le champ d'application du droit communautaire[9]. Toutefois, beaucoup d'États membres, en transposant la directive 95/46/EC, couvrent ces aspects de manière générale, prévoyant, toutefois, des exemptions spécifiques.

**A.** En certains pays, le traitement effectué pour lesdites finalités doit respecter aussi certaines garanties, conformément à la Convention n° 108/1981 et aux Recommandations du Conseil de l'Europe correspondantes, ainsi qu'au sens de dispositions législatives nationales (article 3, paragraphe 2 et considérant n° 16 directive n° 95/46/EC). En raison de son caractère spécifique, ainsi que pour l'existence de dispositions spécifiques connexes également associées à des activités d'investigation effectuées par les autorités de police et/ou judiciaires, ainsi que pour des finalités de sûreté de l'État[10] (qui peuvent inclure la vidéo-surveillance « cachée », c'est à dire sans fournir aucune information sur les endroits surveillés), cette catégorie de traitements n'est pas prise en considération de manière analytique dans ce document.

Toutefois, le groupe de travail souligne qu'il est nécessaire, similairement à ce qui a été noté à propos d'autres traitements de données à caractère personnel qui ne tombent pas dans le champ d'application de la directive, que la vidéo-surveillance justifiée par des exigences réelles de sécurité publique ou de détection, prévention et répression d'infractions, respecte les conditions requises à l'article 8 de la Convention sur les droits de l'homme et les libertés fondamentales. Elle doit en outre être prévue par des dispositions spécifiques connues par le public et être connexe et proportionnée à la prévention de dangers *concrets* et d'infractions *spécifiques* (par exemple, les endroits exposés à des risques réels ou en cas de manifestations publiques qui peuvent raisonnablement être l'occasion pour la commission d'actes criminels)[11]. Les effets produits par les systèmes de vidéo-surveillance doivent être pris en considération (par exemple, le déplacement des activités illicites en d'autres milieux ou secteurs); le responsable du traitement devrait toujours être indiqué de manière claire afin de permettre aux personnes concernées d'exercer leurs droits.

Cette nécessité existe également en raison du fait que des systèmes de vidéo-surveillance sont de plus en plus installés par la police et d'autres autorités publiques (par exemple, autorités locales) et/ou par des organismes privés (banques, associations de sport, sociétés de transport), ce qui comporte le risque de créer une certaine confusion sur les rôles et responsabilités individuelles à l'égard des missions qui doivent être accomplies[12].

[9] Voir considérant n° 16.

[10] On peut faire référence aux principes énoncés par la Cour européenne des droits de l'homme dans l'affaire Rotaru/Roumanie, du 4 mai 2000, ci-dessus mentionné.

[11] Une circulaire française du 22 octobre 1996 citait des endroits isolés ou des établissements ouverts jusqu'à une heure tardive.

[12] Un exemple significatif nous est fourni à ce propos par l'activité menée par des municipalités italiennes afin de contrôler, au moyen de la vidéo-surveillance, des zones publiques où les prostitués sont présentes la nuit. Certaines administrations ont dans le passé déclaré qu'elles étaient compétentes afin de prévenir ce phénomène, tandis que d'autres ont par la suite choisi d'adopter uniquement des ordonnances, interdisant l'arrêt ou le passage des voitures des

**B)** En deuxième lieu, la directive n'est pas applicable aux traitements effectués par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques (article 3, paragraphe 2 et considérant n° 12).

Le fait, par exemple, d'installer un système de vidéo-surveillance pour le contrôle à distance de ce qui se passe exclusivement à l'intérieur d'une habitation privée (pour la prévention de vols ou dans le cadre de la gestion de la "*e-family*"), diffère complètement de la situation qui se crée lorsque la vidéo-surveillance est installée à l'extérieur ou tout près des habitations privées pour la protection de la propriété ou pour garantir la sécurité.

Dans ces cas il est possible que le système ait été installé non par les propriétaires selon un choix individuel de protection des voies d'accès à leur propriété, mais par plusieurs propriétaires en accord entre eux ou par une coopérative ou un regroupement de propriétaires d'unités immobilières, afin de contrôler les entrées ou d'autres espaces en commun, ce qui permet l'application de la directive à cette activité.

De même, lorsque le système est géré à l'avantage d'un seul ménage et pour la prise de vue d'une seule porte, palier, garage, etc., le fait que la directive ne soit pas applicable en raison de l'utilisation exclusivement personnelle du système et de l'impossibilité pour des tiers d'avoir accès aux données, n'exonère pas le responsable du respect des droits et des intérêts légitimes des voisins et d'autres personnes de passage. Ces droits et intérêts sont en tout cas protégés dans les États membres, outre que par les dispositions sur la protection des données, par les dispositions à caractère général de droit civil concernant la protection de la personnalité, de l'image, de la vie familiale et de la vie privée (il suffit de penser, par exemple, au large angle visuel d'une caméra installée à l'extérieur de l'entrée d'une habitation, qui enregistre systématiquement les clients d'un cabinet médical ou d'avocat situé au même étage et qui cause ainsi une ingérence dans le domaine du secret professionnel).

Une attention particulière doit être consacrée à l'orientation des appareils vidéo, à la présence nécessaire de panneaux d'information et à l'effacement rapide des images (depuis quelques heures), lorsque aucune infraction ni aucune effraction n'a été commise.

**C)** Enfin, l'article 9 de la directive établit que les États membres prévoient des exemptions ou des dérogations à certaines des dispositions qui y sont prévues, lorsque le traitement n'est effectué qu'à des fins de journalisme ou d'expressions littéraires ou artistiques, en particulier dans le domaine audiovisuel (considérant n° 17). Il faut prévoir uniquement des exceptions permettant de concilier le droit à la vie privée avec les dispositions réglementant la liberté d'expression[13]. Des précautions particulières s'imposent à cet égard, surtout lors de l'installation de *web-cam* ou de *caméras en ligne*, afin de prévenir des vides ou des zones d'ombre dans le domaine de la protection des personnes faisant l'objet d'une vidéo-surveillance, pour des finalités qui peuvent parfois être de nature publicitaire ou de promotion touristique[14].

---

clients des prostitués et prévoyant l'envoi d'une photo à leur domicile. L'autorité italienne a adopté une disposition afin de spécifier les modalités permettant de contester la relative infraction.

[13] Voir Recommandation 1/97 du groupe de travail sur la loi de protection des données et les moyens de communication.

[14] Une *web cam* qui avait été installée subrepticement près des escaliers d'une sortie du métro de Milan, a transmis directement sur le réseau des parties intimes des femmes de passage, pour des finalités apparemment seulement liées à des activités journalistiques. L'impossibilité de reconnaître les personnes concernées n'a pas permis à l'Autorité nationale de protection des données d'intervenir.

## 6. Vidéo-surveillance et traitement des données à caractère personnel

A la lumière de cette exposition articulée, le groupe estime qu'il est nécessaire d'attirer l'attention sur le fait que la directive n° 95/46/CE est applicable au traitement de données à caractère personnel, y compris les images et les sons récoltés au moyen d'un système CCTV et d'autres systèmes de vidéo-surveillance, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Les images et sons qui se rapportent à des personnes physiques identifiées ou identifiables sont considérés comme des données à caractère personnel :

a) même si les images sont utilisées dans le cadre d'un circuit fermé; même si elles ne sont pas associées aux données d'identité de la personne,
b) même si elles ne concernent pas de personnes dont le visage a été filmé, bien qu'elles contiennent d'autres informations (par exemple, le numéro de la plaque de véhicules ou le *Pin number – Numéro d'Identification Personnelle* - acquis en relation avec la surveillance d'installations pour le prélèvement automatique d'argent-*ATM*),
c) indépendamment du support utilisé pour le traitement, par exemple, systèmes vidéo fixes ou mobiles, tels que les vidéo-récepteurs portables; images en couleur et/ou noir et blanc), de la technique utilisée (dispositifs par câble, dispositifs à fibres optiques), du type d'appareils (fixes, rotatifs, mobiles) des modalités de l'acquisition (continue ou discontinue, par exemple, en cas d'images acquises en cas de violation des limites de vitesse; le cas est différent en cas d'enregistrement d'images effectué de manière occasionnelle et isolée), ainsi que de la communication (la connexion avec un "centre" diffusion d'images vers des terminaux à distance; etc.).

L'identification peut être le résultat, dans les limites imposées par la directive, d'un appariement de données avec des informations gardées par des tiers, ou bien de l'utilisation, dans le cas en question, de techniques particulières ou de dispositifs spéciaux.

Par conséquent, l'une des premières précautions que le responsable du traitement doit respecter est de contrôler si la vidéo-surveillance prévoit ou non un traitement de données à caractère personnel, dans la mesure où elle concerne des personnes identifiables. En ce cas, la directive est applicable même si une disposition spéciale au niveau national prévoit une ultérieure autorisation pour des finalités de sécurité publique.

C'est le cas, par exemple, des installations à l'entrée ou à l'intérieur d'une banque qui permettent l'identification des clients; par contre, dans certaines conditions, la directive pourrait ne pas être applicable en cas de prises de vue aériennes qui ne peuvent être agrandies de manière utile, ou qui ne contiennent pas d'informations relatives à des personnes – comme, par exemple, les prises de vue effectuées sur le territoire, ayant pour objet des sources d'eau ou des déchets, ou pour un contrôle panoramique de la circulation sur les autoroutes.

## 7. OBLIGATIONS ET PRECAUTIONS OPPORTUNES DE LA PART DU RESPONSABLE DU TRAITEMENT

### A) Licéité du traitement

Le responsable doit préalablement vérifier, également en relation avec le principe énoncé à l'article 6, a) de la directive concernant la licéité du traitement, si l'activité de surveillance respecte les dispositions générales et spéciales applicables en la matière (lois, règlements, codes de conduite importants sur le plan juridique). Ces dispositions peuvent être prévues également

pour des finalités de sécurité publique ou pour des finalités autres que celles de protection des données à caractère personnel (par exemple, l'octroi d'une autorisation spécifique par des organismes administratifs particuliers et le respect des prescriptions s'y rattachant).

Il est nécessaire d'adopter toutes les mesures appropriées afin de garantir que la vidéo-surveillance sera conforme aux principes sur la protection des données, ainsi que d'éviter toute référence non appropriée à la vie privée[15].

Il est opportun à ce propos de tenir compte également d'éventuelles dispositions de bonne pratique prévue par des recommandations émanant d'autorités de contrôle, ainsi que d'autres dispositions d'autodétermination.

De même, il est nécessaire de vérifier les dispositions normatives prévues par la législation nationale en vigueur (normes constitutionnelles; dispositions des codes civil et pénal), en particulier en ce qui concerne le "droit à l'image"[16] ou la protection du domicile, en tenant compte de la jurisprudence qui, dans certains cas, peut avoir établi que certains locaux, autres que ceux de l'habitation privée, peuvent être considérés comme le domicile d'une personne (par exemple, chambres d'hôtel, bureaux, salles de bains, vestiaires, postes téléphoniques internes, etc.).

Si l'équipement a été installé par des particuliers ou par des administrations publiques, surtout au niveau local, pour des finalités de sécurité ou de détection, prévention et répression d'infraction, il est nécessaire, lorsque lesdites finalités sont déterminées et communiquées, de considérer avec attention les compétences pouvant être licitement exercées par le responsable du traitement. Il faudra tenir compte des fonctions publiques qui ne peuvent être exercées, aux termes de la loi, que par des organismes spécifiques non administratifs tels que, en particulier, des organismes de police et/ou l'autorité judiciaire.

Le problème se pose de manière spécifique à l'égard de certaines collectivités communales et provinciales, qui n'ont pas de compétence directe en matière d'ordre et de sécurité publique, mais qui toutefois exercent des activités auxiliaires à des fins de surveillance. De même, il y a des activités de surveillance qui, en certain cas, sous prétexte de réprimer les infractions, visent en réalité à prédisposer des éléments de preuve en cas de commission d'actes illicites.

**B) Détermination, définition et licéité des finalités**

Le responsable doit agir afin que les finalités recherchées ne soient ni incertaines ni ambiguës, et ce également afin de pouvoir disposer d'un critère précis au moment de l'application du principe de compatibilité, des buts poursuivis dans le traitement (article 6, b), de la directive).

Cette clarification est également nécessaire pour pouvoir énoncer de manière claire les finalités, non seulement dans les informations à fournir aux personnes concernées, mais aussi dans la notification correspondante, ainsi que dans le cadre d'un éventuel contrôle préliminaire du traitement, effectué en application de l'article 20 de la directive.

Toute utilisation ultérieure des images récoltées devrait être exclue, avec une attention particulière en ce qui concerne la possibilité technique de reproduction (par exemple, interdiction expresse d'effectuer des copies).

[15] Tout récemment, une banque et une autorité locale de police n'ont pas donné suite à la requête formulée par un client victime d'un vol, demandant que soient extraites des images enregistrées par une caméra qui filmait, entre autres, un guichet automatique, celles relatives au voleur qui, après avoir volé sa carte bancaire, l'avait illicitement utilisée au guichet, et ce, pour des raisons présumées de « protection de la vie privée ».

[16] Ce droit prévoit en France et en Belgique un 'consentement préalable'.

Ces finalités devraient être mentionnées dans un document qui devrait résumer d'autres aspects importants de la *privacy policy*, en faisant aussi référence à certains aspects importants tels que l'indication du moment de l'effacement des images et les requêtes d'accès et/ou de consultation éventuellement présentées par les personnes concernées.

## C) Critères de légitimation du traitement

Le responsable doit s'assurer que la vidéo-surveillance respecte non seulement les dispositions spécifiques précédemment mentionnées en A), mais aussi, en ce qui concerne la protection des données à caractère personnel, au moins l'une des conditions qui rendent le traitement licite, en vertu de l'article 7 de la directive.

A l'exclusion des cas moins fréquents qui exigent l'accomplissement d'une obligation de loi (par exemple, certains casinos) ou lorsque le traitement est nécessaire pour protéger des intérêts prioritaires (le contrôle à distance des patients en soins intensifs), le responsable doit souvent faire face à la nécessité d'accomplir une mission d'intérêt public ou connexe à l'exercice de pouvoirs publics, laquelle peut éventuellement être réglementée par des dispositions spécifiques (par exemple : détection d'infractions au code de la route, détection d'agressions à l'intérieur des moyens de transport publics en des zones intéressées par un haut taux de criminalité : article 7, e); par contre, le responsable peut avoir la nécessité de poursuivre un intérêt licite par rapport auquel ne prévalent pas les intérêts ni les droits et libertés fondamentales de la personne concernée (article 7, f).

Dans ces deux cas, en particulier dans le deuxième, le caractère sensible du traitement exige une analyse rigoureuse des compétences, pouvoirs et intérêts licites du responsable du traitement. Il faut absolument éviter toute considération superficielle ou basée sur des interprétations qui étendent de manière arbitraire le champ de ces compétences et pouvoirs.

En cas d'équilibre entre les intérêts concernés, il faudra examiner avec une particulière attention, aussi en écoutant préalablement les parties concernées, la possibilité qu'un intérêt des personnes concernées qui mérite d'être protégé soit en contraste avec l'installation du système ou avec des modalités particulières relatives à la conservation ou encore avec d'autres opérations du traitement[17].

Enfin, le consentement de la personne concernée, s'il est requis, doit être donné de manière non ambiguë et sur la base d'informations claires. Un consentement spécifique doit être donné séparément pour des activités de surveillance de lieux où se déroule la vie privée de la personne concernée[18].

Une évaluation de la licéité du traitement doit être également effectuée en tenant compte des dispositions prévues par la directive prévoyant des garanties spécifiques pour les données concernant les infractions (article 8, paragraphe 5, directive)[19].

---

[17] L'article 6b de la nouvelle loi fédérale allemande, entrée en vigueur le 23 mai 2001, prévoit la possibilité d'effectuer une surveillance de certains lieux accessibles au public au moyen d'équipements optiques ou électroniques, à condition qu'il n'existe pas, entre autres, des raisons de penser que les intérêts de la personne concernée qui méritent d'être protégés sont prioritaires par rapport à la surveillance.

[18] Une attention particulière doit être accordée à la possibilité réelle d'exprimer un consentement valable au sens de l'article 2, point h) de la directive 95/46/CE ("toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement" en cas d'installation d'un système de vidéo-surveillance en co-propriété (résidences en co-propriété, etc.).

[19] Un exemple est fourni par les dispositions de l'article 8 de la loi portugaise n° 67/98 relatives aux données concernant des personnes suspectées de participer à des activités illicites ou criminelles.

Des mesures et des dispositions supplémentaires pourraient résulter de l'évaluation préliminaire du traitement en application du mécanisme de contrôle préalable si la vidéo-surveillance présente des risques particuliers au regard des droits et libertés des personnes concernées (article 20 de la directive 95/46/CE).
Le traitement effectué au moyen de la vidéo-surveillance devrait en tout état de cause être prévu par une expresse disposition législative, lorsqu'il est opéré par un organisme public.

**D) Proportionnalité dans le recours à la vidéo-surveillance**

Le principe selon lequel les données doivent être adéquates et pertinentes par rapport aux finalités poursuivies comporte, avant tout, que les systèmes CCTV et les autres dispositifs similaires de vidéo-surveillance ne peuvent être mis en place que sur une base de subsidiarité, c'est à dire :

Lorsqu'il existe des finalités justifiant effectivement le recours auxdits systèmes.

Selon le principe de proportionnalité, ces systèmes peuvent être mis en œuvre si d'autres mesures de prévention, de protection et/ou de sécurité de nature physique et/ou logique ne requérant aucune acquisition d'images, telles que, par exemple, le blindage des portes pour protéger du vandalisme, l'installation de barrières automatiques et de dispositifs d'autorisation d'accès, de systèmes d'alarme communs, l'amélioration et le renforcement de l'éclairage des rues, etc. s'avèrent manifestement insuffisants et/ou inapplicables pour poursuivre lesdites finalités licites.

Le même principe s'applique au choix de la technologie appropriée, aux critères d'utilisation de l'équipement dans des cas concrets et à la spécification des dispositions en matière de traitement des données, en ce qui concerne les règles d'accès et la période de rétention.

En d'autres mots, il est nécessaire d'appliquer, au cas en examen, le *principe* selon lequel les données doivent être adéquates par rapport aux finalités recherchées, qui comporte une sorte "*d'obligation d'intervention minimum"* par le responsable.

Par conséquent, l'installation d'un système proportionné de vidéo-surveillance et d'alarme connexe peut être considérée comme licite si plusieurs épisodes de violence se produisent dans une zone proche d'un stade ou en cas d'agressions répétées en des zones périphériques à bord ou dans les voisinages des arrêts des autobus. Par contre, la situation est différente en ce qui concerne des systèmes visant à détecter (comme il a été requis à une autorité de contrôle des données), les responsables d'insultes envers le conducteur ou de graffitis à l'extérieur des autobus (qui ne seraient d'ailleurs pas enregistrés par les caméras installées à bord), à identifier des citoyens responsables uniquement d'infractions administratives de moindre importance, par exemple, le fait de jeter la poubelle sur la rue ou en des zones interdites ou à détecter les personnes responsables de vols occasionnels dans les piscines.

L'évaluation de la proportionnalité doit être encore plus rigoureuse lorsque les endroits ne sont pas accessibles au public.

Un échange d'informations et d'expériences entre les autorités compétentes des différents États membres pourrait se révéler très utile[20];

[20] Ceci pourrait aider à harmoniser davantage les approches normatives et les décisions administratives qui devront être adoptées et qui, dans certains cas, ont été dans le passé très divergentes (voir, par exemple, les salles de Bingo).

Ces considérations sont surtout applicables aux cas toujours plus fréquents de vidéo-surveillance installée pour des finalités d'autodéfense et de protection des biens, en particulier, à proximité d'immeubles et de bureaux publics, y compris les zones qui les entourent. A ce propos, une évaluation plus générale des effets indirects d'un recours massif à la vidéo-surveillance s'impose (réelle efficacité de dissuasion découlant de l'installation de plusieurs systèmes; déplacement en d'autres zones des activités de vandalisme ou d'autres activités illicites, etc.).

## E) Proportionnalité dans le déroulement des activités de vidéo-surveillance

Le principe selon lequel les données doivent être adéquates, pertinentes et non excessives comporte, après l'évaluation positive sur la licéité du traitement de données opéré au moyen de la vidéo-surveillance, une évaluation approfondie de la *proportionnalité des modalités* dudit traitement.

*Les modalités de prise de vue* doivent être examinées, en tenant compte en particulier des aspects suivants :

a) l'angle de prise de vue par rapport aux finalités poursuivies[21] (par exemple, en cas de surveillance en des lieux publics, l'angle ne doit pas permettre la vision des détails ou des traits somatiques qui ne sont pas importants pour les finalités recherchées : détails de véhicules ou des conducteurs, ou bien de l'intérieur de lieux privés qui se trouvent à proximité, surtout en cas d'utilisation des fonctions zoom);
b) le type des dispositifs de prise de vue utilisés (fixes ou mobiles);
c) leur installation (localisation des caméras ; utilisation de caméras fixes et/ou mobiles);
d) la possibilité d'agrandir les images ou d'utiliser la fonction zoom déjà au moment de la prise de vue ou bien *a posteriori*, sur des images conservées et la possibilité de brouiller ou de supprimer des images individuelles;
e) la fonction d'arrêt sur image;
f) la connexion avec un "centre" auquel on peut transmettre des signaux d'alarme sonores ou visuels;
g) les mesures adoptées sur la base de la vidéo-surveillance (fermeture de voies d'accès, intervention du personnel de surveillance, etc.).

En deuxième lieu, il est nécessaire de prendre en considération les *décisions qui doivent être adoptées en ce qui concerne la conservation éventuelle des images et la période de conservation*; cette période doit être très brève et articulée selon les caractéristiques spécifiques du cas en examen.

Si, dans certains cas, un système prévoyant la seule vision en circuit fermé des images, et qui exclut l'enregistrement, peut être suffisant (la caisse d'un grand magasin, par exemple) par contre, en d'autres cas (pour la protection d'immeubles privés), il pourrait être justifié de conserver les images pendant quelques heures et de les effacer automatiquement à la fin de la journée au maximum et au moins à la fin de la semaine. Une exception à cette règle peut être prévue lorsqu'il existe un motif raisonnable d'attendre, pour un temps déterminé,

[21] Des exemples de précautions adoptées par rapport à l'angle visuel peuvent être fournis par deux décisions de l'Autorité italienne pour la protection des données à caractère personnel. Un organisme de santé, qui désirait installer un service permettant aux familiers d'observer à distance de manière continue les patients en état de coma, en isolement ou en une unité de soins intensifs, a souligné la nécessité d'utiliser des dispositifs appropriés pour éviter la vision simultanée d'autres patients. Dans un autre cas, l'Autorité a souligné la nécessité aux organismes administratifs de police, que le système de détection d'excès de vitesse enregistre uniquement la plaque et non l'intérieur des voitures.

l'éventuelle décision de l'autorité judiciaire ou de police si, par exemple, une alarme a été lancée ou qu'une requête digne d'être prise en considération a été faite.

Toujours à titre d'exemple, un système finalisé à détecter uniquement les accès non autorisés de véhicules aux centres ville et à des zones à circulation limitée, ne devrait enregistrer les images que lorsqu'une infraction a été commise.

Le problème de la proportion doit être pris en considération de manière scrupuleuse aussi lorsqu'il existe des exigences de conservation des images pour une période moins brève, mais qui ne doit pas dépasser une semaine[22] au maximum (par exemple : vidéo-surveillance près les établissements bancaires, pour identifier les fréquentant les locaux d'une banque dans les jours qui ont précédé l'exécution d'un vol).

En troisième lieu, il faut examiner avec attention le cas où il est possible *d'identifier une personne est facilitée* en raison de l'appariement des images du visage et d'autres informations relatives à des actions ou comportements enregistrés (c'est le cas de l'appariement des images avec des opérations effectuées par des clients dans une banque à un moment qui est facilement identifiable).

À ce propos, il est nécessaire d'analyser l'incontestable différence qui existe entre, d'une part, la conservation temporaire des images obtenues par un système de vidéo-surveillance installé à l'entrée d'une banque et, d'autre part, la création de banques de données ayant pour objet des photos et des empreintes digitales des clients d'une banque, lesquels y ont consenti, et qui exercent une ingérence bien plus importante sur la vie privée.

Enfin, une particulière attention doit être consacrée aux choix qui doivent être adoptés pour ce qui est de la *possible communication des données aux tiers* (en principe, cette communication ne devrait pas avoir pour objet ceux qui ne sont pas concernés par l'activité de surveillance) ou la diffusion totale ou partielle à l'étranger ou *on-line* de ces données (en considération aussi des dispositions sur la protection adéquate : article 25 et articles suivants).
Il est évident que le principe selon lequel les images acquises doivent être pertinentes et non excessives, est applicable également par rapport à l'éventuel appariement d'informations gardées par plusieurs responsables de systèmes de vidéo-surveillance.

Ces garanties mettent en œuvre, aussi sur le plan opérationnel, ce que certaines dispositions internes considèrent comme *le principe de modération dans l'utilisation des données à caractère personnel*, qui a pour but d'éviter ou de réduire au maximum le traitement de ces données.

Ce principe doit être appliqué dans tous les secteurs, en tenant compte du fait que nombre de finalités qui, à toute première vue, sembleraient nécessiter de données à caractère personnel, peuvent en réalité être atteintes sans avoir recours à ces données, ou en utilisant des données réellement anonymes.

Ces considérations sont applicables également lorsqu'il existe la nécessité justifiée de rationaliser les ressources d'entreprise[23] ou d'améliorer les services offerts aux utilisateurs[24].

[22] Les autorités danoises et suédoises chargée de la protection des données ont émis l'avis que les enregistrements vidéo ne peuvent être stockés que pour une brève période ne dépassant pas 30 jours.
[23] C'est le cas, par exemple, de la nécessité de déterminer le nombre des caisses qui doivent rester ouvertes contemporainement dans un supermarché selon l'affluence des clients, ainsi que de la création d'un « parcours d'achat » optimal pour les consommateurs.

## F) Informations données aux personnes concernées.

Les principes de transparence et de loyauté dans l'utilisation des dispositifs de vidéo-surveillance prévoient que les informations données aux personnes concernées seraient adéquates, conformément aux dispositions énoncées aux articles 10 et 11 de la directive.

Ces personnes doivent être informées au sens des articles 10 et 11 de la directive. Elles doivent être conscientes du fait que des activités de vidéo-surveillance sont en cours, également lorsqu'elles sont effectuées à l'occasion de spectacles ou d'événements publics (stades), ou encore d'activités publicitaires (*web-cam*); elles doivent en outre être informées de manière ponctuelle sur les lieux mis sous surveillance.

Il n'est pas nécessaire de spécifier exactement le point où les dispositifs ont été installés; toutefois, il faut indiquer de manière non ambiguë l'endroit surveillé.

Les panneaux d'information doivent être placés de manière stable à une distance non excessive des endroits surveillés (dans certains cas, on a déjà admis une distance de 500 mètres); les installations doivent être situées à une distance raisonnable selon le type de prise de vue.

Les panneaux d'information doivent être visibles et synthétiques, à condition qu'ils soient efficaces; ils peuvent inclure également des symboles déjà utilisés en relation avec la vidéo-surveillance et avec les panneaux de défense de fumer (ils peuvent être différents selon que les images sont enregistrées ou non). Ils doivent indiquer les finalités des activités de surveillance ainsi que le responsable du traitement. Les dimensions des panneaux doivent être proportionnées aux lieux[25].

Des restrictions spécifiques et motivées concernant l'obligation d'information ne peuvent être prévues que dans les seules limites visées aux articles 10, 11 et 13 de la directive (par exemple, une limitation temporaire peut être prévue pour les données récoltées à des fins licites d'investigation de la défense ou, conformément à la loi, afin d'exercer le droit à la défense, pendant la seule période où cela porterait atteinte aux finalités poursuivies).

Enfin, une attention particulière doit être accordée aux moyens appropriés de fournir l'information aux personnes non voyantes...

## G) Conditions supplémentaires requises

En ce qui concerne les autres conditions, précautions et garanties prévues par les dispositions sur la protection des données à caractère personnel et synthétisés au point 3 (en faisant référence aussi à la nécessité que les traitements de données à caractère personnel soient notifiés et assujettis au contrôle d'une autorité indépendante, conformément aux articles 18, 19 et 28 de la directive), le groupe appelle l'attention en particulier sur les aspects qui suivent.

a) Il faut indiquer les personnes physiques, en nombre limité, qui peuvent visionner ou avoir accès aux images éventuellement enregistrées, pour les seules finalités poursuivies au moyen de la vidéo-surveillance, ou bien pour des nécessités liées à l'entretien des

[24] Pour faciliter l'entrée dans un lieu de travail ou à bord d'un moyen de transport spécifique, s'il existe la nécessité d'un contrôle d'identité, il suffit d'utiliser des cartes d'identité avec photo de la personne concernée, possiblement sur support informatique, évitant l'installation d'un système de reconnaissance de visage.

[25] Ce que l'on pourrait qualifier d'approche «à plusieurs niveaux »

dispositifs afin d'en vérifier le bon fonctionnement, ou encore à la suite d'une requête présentée, au sens de la loi, par la personne concernée ou par l'autorité de police ou judiciaire en vue de la détection d'infractions.

Lorsque la finalité poursuivie ne concerne que la détection, la prévention et la répression d'infractions, la solution de la double clé d'accès aux images enregistrées (l'une gardée par le responsable et l'autre par la police) peut se révéler utile dans de nombreux cas afin de garantir que les images ne seront visionnées que par les autorités de police et non par le personnel, sans préjudice de l'exercice du droit d'accès de la part de la personne concernée sur requête présentée pendant la brève période de conservation des images.

b) Des mesures de sécurité appropriées doivent être adoptées afin d'éviter que l'une des circonstances prévues à l'article 17 de la directive puisse avoir lieu, y compris la dissémination d'informations qui peuvent être utiles aux fins de protection d'un droit de la personne concernée, de tiers ou du responsable du traitement. Ces mesures doivent en outre éviter toutes manipulations, altérations ou destructions de données et d'éléments de preuve associés.

c) Il est essentiel que les images enregistrées soient de bonne qualité, en particulier si les mêmes supports sont fréquemment réutilisés, ce qui comporte le risque que des images précédentes n'aient pas été effacées de manière appropriée.

d) Pour terminer, une importance particulière doit être accordée aux activités de formation et de sensibilisation continue des opérateurs qui sont concrètement chargés de ces activités, surtout en ce qui concerne le respect des obligations en la matière. De même, la formation des contrôleurs et des opérateurs en ce qui concerne les risques associés et les mécanismes permettant d'identifier les individus photographiés ou filmés, peut être considérée comme une mesure utile.

## H) Droits des personnes concernées

La nature particulière des données à caractère personnel récoltées n'exclut pas que les personnes concernées puissent exercer les droits prévus aux articles 13 et 14 de la directive, en particulier le droit de s'opposer au traitement. La directive 95/46 autorise effectivement la personne concernée à s'opposer à tout moment au traitement de données à caractère personnel[26] pour des raisons prédominantes et licites relatives à sa situation particulière.

Le droit des personnes concernées à l'oubli et la conservation généralement limitée des images limite le champ d'application du droit d'accès de la personne aux données à caractère personnel qui la rendent tout au moins identifiable. Ce droit doit toutefois être garanti surtout lorsqu'il y a une requête détaillée permettant de retrouver l'image aisément, compte tenu également de la nécessité de sauvegarder l'intérêt de tierces personnes aussi de manière temporaire.

Toute éventuelle restriction applicable lorsque les efforts qui doivent être entrepris pour rechercher les images se révèlent manifestement disproportionnés en termes de recherches, de coûts et de ressources, du fait de la courte durée de la période de conservation de ces images, ne devrait être prévue que par une disposition de loi (article 13, paragraphe 1 de la

[26] Sauf si la législation nationale en dispose autrement.

directive). Il sera tenu compte du droit de défense de la personne concernée par rapport à des événements spécifiques qui ont eu lieu pendant la période prise en considération.

### I) Garanties supplémentaires relatives à des traitements particuliers

La vidéo-surveillance effectuée *uniquement* pour des raisons ayant trait à l'appartenance raciale, aux convictions religieuses, politiques ou syndicales ou à des comportements sexuels déterminés d'un groupe de personnes, doit être interdite (article 8 de la directive).

Le groupe, n'ayant pas l'intention de rédiger dans ce contexte une liste exhaustive des différentes applications découlant de la pratique, désire appeler l'attention sur la nécessité de considérer attentivement et en ligne générale, où cela est possible, dans le cadre du contrôle préliminaire des traitements opérés au sens de l'article 20 de la directive, certains contextes dans lesquels des images concernant des personnes identifiées ou identifiables ont été acquises et qui demandent une analyse spécifique, selon le cas en figure.

Il s'agit, en particulier, des situations qui suivent et qui découlent d'expériences ou de pratiques déjà en cours :

a) interconnexion permanente de systèmes de vidéo-surveillance opérés par différents responsables;
b) éventuelle association d'images avec des données biométriques, telles que les empreintes digitales (par exemple, à l'entrée des banques);
c) utilisation de systèmes permettant d'identifier la voix;
d) adoption, conformément aux principes de proportionnalité et sur la base de dispositions spécifiques, de systèmes d'indexation des images enregistrées et/ou de recherche automatisée desdites images, surtout au moyen de données d'identité;
e) utilisation de systèmes de reconnaissance du visage qui ne se limitent pas simplement à reconnaître le camouflage de personnes de passage (fausses barbe ou perruque), mais qui se basent sur des techniques permettant de signaler les personnes suspectes. Il s'agit de la possibilité pour le système de reconnaître automatiquement des personnes sur la base de clichés et/ou de kits d'identité basés sur des signes extérieurs spécifiques (couleur de la peau, couleur des yeux, traits du visage, etc.), ou bien sur des comportements « anormaux » prédéterminés (mouvements brusques, passages successifs de la personne suspecte à des intervalles déterminés, manière de garer la voiture). A cet égard, l'intervention d'un opérateur est opportune, aussi à la lumière des possibles erreurs qui pourraient avoir lieu dans ces cas, comme mentionné en f);
f) possibilité de tracer automatiquement des parcours et des trajets et/ou de reconstruire ou prévoir les comportements d'une personne;
g) adoption de décisions automatisées basées sur un profile de la personne ou sur des systèmes intelligents d'analyse et d'intervention ne découlant pas des normales situations d'alarme (accès sans identification, alarme d'incendie, etc.).

## 8. Vidéo-surveillance sur les lieux de travail

Dans l'*avis° 8/2001 sur le traitement de données personnels dans le milieu du travail* adoptée le 13 septembre 2001, ainsi que dans le *document de travail concernant la surveillance des communications électroniques sur le lieu de travail*, adopté le 29 mai 2002[27], le groupe a déjà

[27] Ces deux documents sont disponibles à l'adresse suivante:
http://www.europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm.

appelé l'attention sur un certain nombre de principes applicables à la protection des droits, des libertés et de la dignité des personnes concernées sur les lieux de travail.

En plus des observations faites dans ces documents et des applications concrètes à la vidéo-surveillance, il est nécessaire que les systèmes de vidéo-surveillance ayant comme finalité directe le contrôle à distance de la qualité du travail et de la productivité, et qui comportent donc le traitement de données à caractère personnel dans ce contexte, soient de règle interdite.

Par contre, s'il existe des garanties appropriées, les systèmes vidéo justifiés par des réelles exigences de production ou de sécurité du travail pourraient être admis, bien qu'ils puissent avoir comme effet indirect le contrôle à distance[28].

L'expérience concernant l'application de la surveillance met en évidence la nécessité que des endroits réservés aux travailleurs et qui ne sont pas destinés à une activité de travail (toilettes, douches, vestiaires et zones de repos) ne soient pas soumis à surveillance; que les images récoltées à des fins exclusives de défense de la propriété et de détection, prévention et répression d'infractions graves, ne soient pas utilisées pour contester au travailleur des infractions disciplinaires de moindre importance; que le droit pour les travailleurs de s'opposer en utilisant les images enregistrées soit garanti.

Des informations doivent être fournies aux salariés et à toute autre personne travaillant sur les lieux. Ces informations doivent inclure l'identité du contrôleur et l'objet de la surveillance ainsi que d'autres renseignements nécessaires pour garantir un traitement équitable concernant les personnes sur lesquelles sont recueillies des données, par exemple dans quels cas des enregistrements seront examinés par la direction de l'entreprise, la période d'enregistrement et la date à laquelle l'enregistrement sera communiqué aux représentants de la loi. La communication des 'informations, par le biais d'un symbole, par exemple, ne peut être jugée suffisante dans le contexte de l'emploi.

## 9. Conclusions

Le groupe de travail a rédigé ce document de travail pour donner son apport en vue de l'application uniforme des mesures nationales adoptées au sens de la directive 95/46/CE dans le domaine de la vidéo-surveillance.

*** * ***

Dans ce contexte, il est essentiel que les Etats membres orientent les activités des producteurs, des revendeurs et des fournisseurs de services, ainsi que des chercheurs, pour que l'évolution des technologies, des logiciels et des dispositifs techniques soit conforme aux principes énoncés dans ce document.

*** * ***

[28] Dans de tels cas, parallèlement à l'ensemble des observations faites dans le présent document, il conviendrait également de tenir compte de la nécessité de respecter les droits prévus par des accords collectifs. Ces accords reposent, parfois, sur une information collective des travailleurs ou de leurs organisations syndicales (indépendamment des informations prévues sur base individuelle par la législation sur la protection des données) ; en d'autres cas, un accord préalable doit être recherché avec des représentants de travailleurs ou avec leurs organisations syndicales ayant pour objet les modalités d'installation, y compris par rapport à la durée de la surveillance et à d'autres détails concernant les prises de vue. En certain pays, il est prévu l'intervention de l'Etat, si les parties ne parviennent à un accord.

Fait à Bruxelles,
Par le groupe de travail
Le Président
Stefano RODOTA