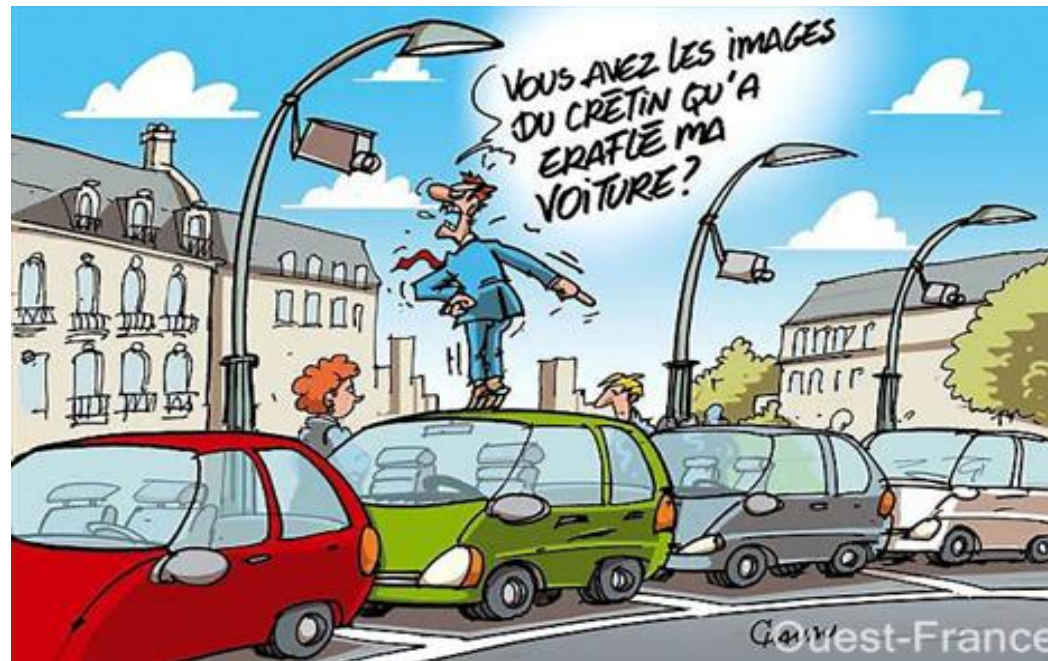




# INTRO : Réglementation

→ La Vidéo surveillance



- **Le clip du groupe The Get Out Close auraient été tourné à partir de caméras de surveillance de Manchester. Mais la vérité différerait légèrement des dires du groupe...**
- Il y a 5 mois, un groupe indépendant de Manchester cherchait à tourner un clip à moindre frais, tout en restant original. Comme la loi les y autorise, ils ont décidé d'utiliser les caméras de surveillance de la ville de Londres, afin de récupérer toutes les images sur lesquels ils apparaissaient. L'idée était novatrice et surtout peu coûteuse.



- Il ne s'agit pas d'être pour ou contre une technologie, mais d'avoir une interrogation sur ces usages.
- Dans le cas de la vidéosurveillance, ce qui nous interpelle **c'est le risque de l'usage de l'image numérique**. La focalisation sur la vidéosurveillance est démonstrative, mais mal fondée, car en matière de traçage informatique il existe aujourd'hui de nombreux systèmes nomades qui nous tracent en permanence, alors qu'ils sont dédiés à des **finalités** simples de communications !!!
- Ce **capital identitaire** sous toutes ses formes, donnée, image ou son, appartient à notre **patrimoine privé**, et chacun doit pouvoir en assurer **l'exactitude dans le temps**. A ce titre, une image ne peut être sortie de son contexte (**finalité**) sans atteinte aux libertés. Nous sommes bien dans un besoin de sécurité, garantir **l'immunité de l'information** dans le temps.
- *Le droit doit préserver et prévenir avant de sanctionner, et se nourrir de l'expérience, or le cycle du progrès technologique actuel perturbe ce processus.*

- Attaques dans les mondes virtuels
  - Détournement des données personnelles sur les réseaux sociaux
  - Attaques en réputation et espionnage industriel en ligne
- 
- **Attention à la new TEC Paranoïa**
  - **Le «prédateur» est toujours le même, + la new TEC**
- 
- **Desidentité, Indélébilité , Irresponsabilité**

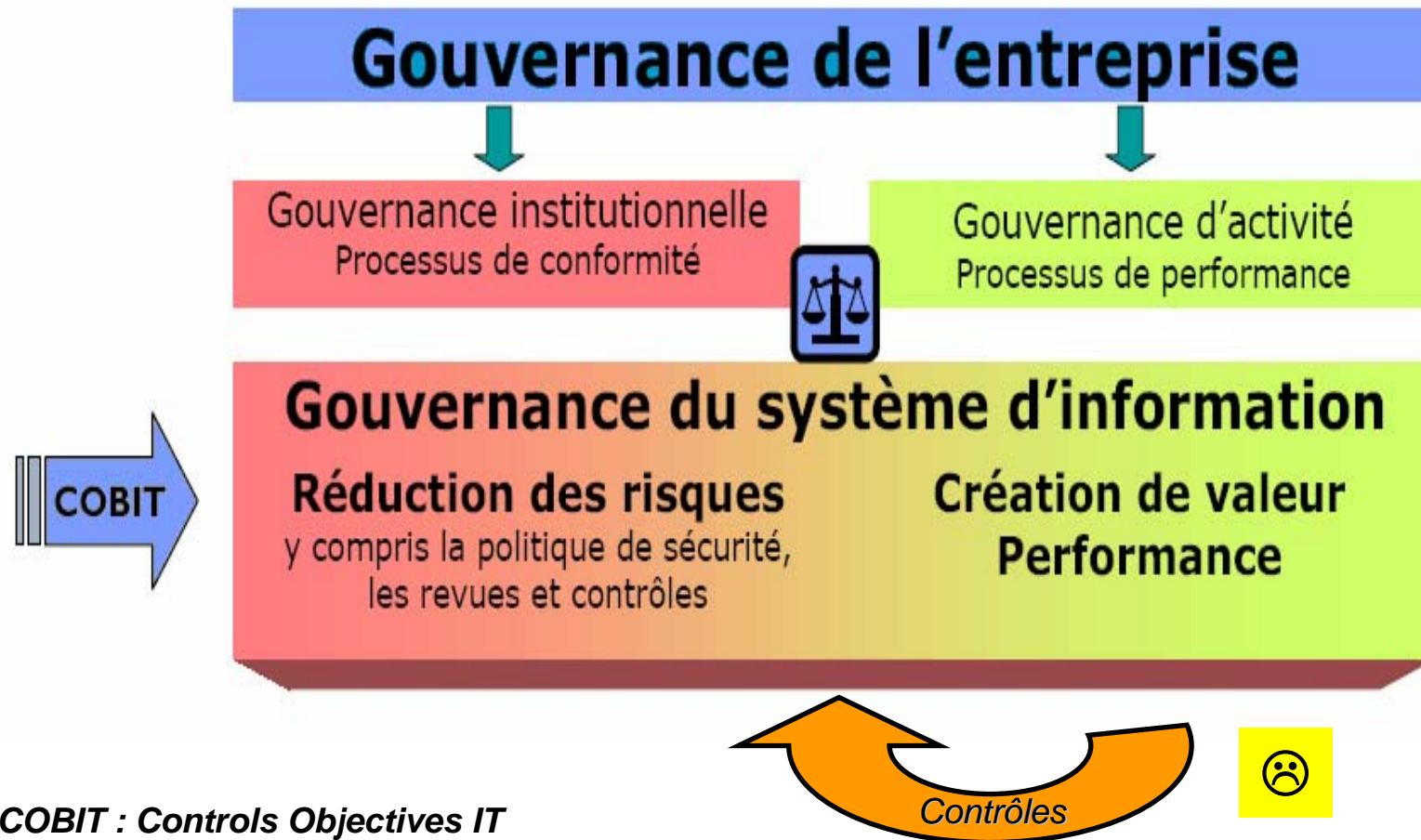
## ■ Article 1er

*L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*

- La **finalité** du système automatisé
- La **proportionnalité** du traitement des données « *nominatives* »
- La pertinence des données ....
- La durée de conservation des données ...
- La sécurité des données ...
- La **transparence**
- Le droit des employés (ou candidats)



**Loyauté**  
**Transparence**  
**Proportionnalité**



## Vidéo Surveillance : TEXTES DE REFERENCE :

---

- Article 10 de la loi du 21/01/1995 sur la prévention de l'insécurité modifié par la loi n° 2006-64 du 23/01/2006
- Décret n° 96-926 du 17/10/1966, modifié par décret n°2006-929 du 28/07/2006, relatif à la Vidéosurveillance
- Arrêté du 3/08/2007, portant définition des normes techniques des systèmes de vidéosurveillance et abrogeant l'arrêté du 26septembre 2006
- Circulaires ministérielles du 22/10/1996 et du 26/10/2006
- L'article 10 de la loi 95-73 du 21/01/1995 modifié par la loi 2006-64 du 23/01/2006 stipule que **les enregistrements visuels de vidéosurveillance ne sont pas de la compétence de la Commission Nationale de l'Informatique et des Libertés (C.N.I.L).**
- Ils sont soumis à **autorisation préfectorale** après avis de la commission départementale de vidéosurveillance. **L'arrêté préfectoral est valable 5 ans.**

## Vidéo surveillance : CHAMP D'APPLICATION :

### ■ Sont concernés :

- tous les systèmes de vidéosurveillance, que le dispositif technique fasse appel aux techniques analogiques ou numériques ;
- le simple visionnage d'images transmises à un poste central sans dispositif d'enregistrement ;
- la transmission et l'enregistrement des images, mais seulement dans le cas où ces images ne sont pas utilisées pour alimenter un fichier nominatif.

### ■ Ne sont pas concernés :

- les systèmes dans lequel il n'y a ni enregistrement, ni même une simple transmission des images (exemple : écrans de visualisation installés à la vue de tous).

→ ***L'installation d'un système de vidéosurveillance ne doit pas porter atteinte à la vie privée d'autrui. Les clients et usagers doivent être clairement avertis de la présence de caméras et/ou d'un dispositif d'enregistrement. (système de surveillance vidéo)***

→ ***De la même façon, que vous utilisiez des caméras à domicile, à titre privé ou dans des locaux professionnels, vous devez également en avertir toute personne ayant avec vous un lien de subordination non familial.***

- L'installation d'un système de vidéosurveillance sur la voie publique est autorisée par arrêté préfectoral et par une autorité publique compétente dans les cas suivants :
  - la protection des bâtiments et installations publics et de leurs abords,
  - la sauvegarde des installations utiles à la défense nationale,
  - la régulation du trafic routier, la constatation des infractions aux règles de la circulation
  - la prévention des atteintes à la sécurité des personnes et des biens dans les lieux particulièrement exposés à des risques d'agression ou de vol.
  - Les opérations de vidéosurveillance de la voie publique sont réalisées de telle sorte qu'elles ne visualisent pas les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées.
  - L'installation d'un système de vidéosurveillance peut également être réalisée dans des lieux et établissements ouverts au public et particulièrement exposés à des risques d'agression ou de vol, aux fins d'y assurer la sécurité des personnes ou des biens.
- **Le public doit être informé de manière claire et permanente** de l'existence du système de vidéosurveillance et de l'autorité ou de la personne responsable.

- demande sur imprimé CERFA [10426\\*01](#)
- lettre de motivation exposant la finalité du système vidéo et justifiant son utilité ;
- plan de détail à une échelle suffisante montrant le nombre et l'implantation des caméras ainsi que les zones couvertes par celles-ci ;
- plan de masse des lieux montrant le ou les bâtiments (si caméras à l'extérieur) ;
- descriptif du matériel utilisé. Ce matériel doit être conforme au descriptif mentionné dans l'arrêté du 03/08/2007 ;
- modèle de l'affichette qui sera apposée pour informer la clientèle que l'établissement est placé sous vidéosurveillance.
- Dès réception du dossier complet en Préfecture, un récépissé est délivré et adressé en Recommandé avec Accusé de Réception au pétitionnaire.
- Le Préfet dispose ensuite d'un **délai de quatre mois maximum** pour soumettre le dossier à la Commission Départementale de Vidéosurveillance.

Le fait de procéder à des enregistrements de vidéosurveillance :

- sans autorisation ;
  - de ne pas les détruire dans le délai prévu ;
  - de les falsifier ;
  - d’entraver l’action de la commission départementale ;
  - de faire accéder des personnes non habilitées aux images ;
  - d’utiliser les images à d’autres fins que celles pour lesquelles elles sont autorisées ;
- est puni de **3 ans d’emprisonnement et de 45 000 € d’amende**, sans préjudice des dispositions des articles 226-1 du Code Pénal et L.120-2, L.121-8 et L.432-2-1 du Code du Travail.

Code Pénal Articles 226-16 à 24

## **Section 5 Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques**

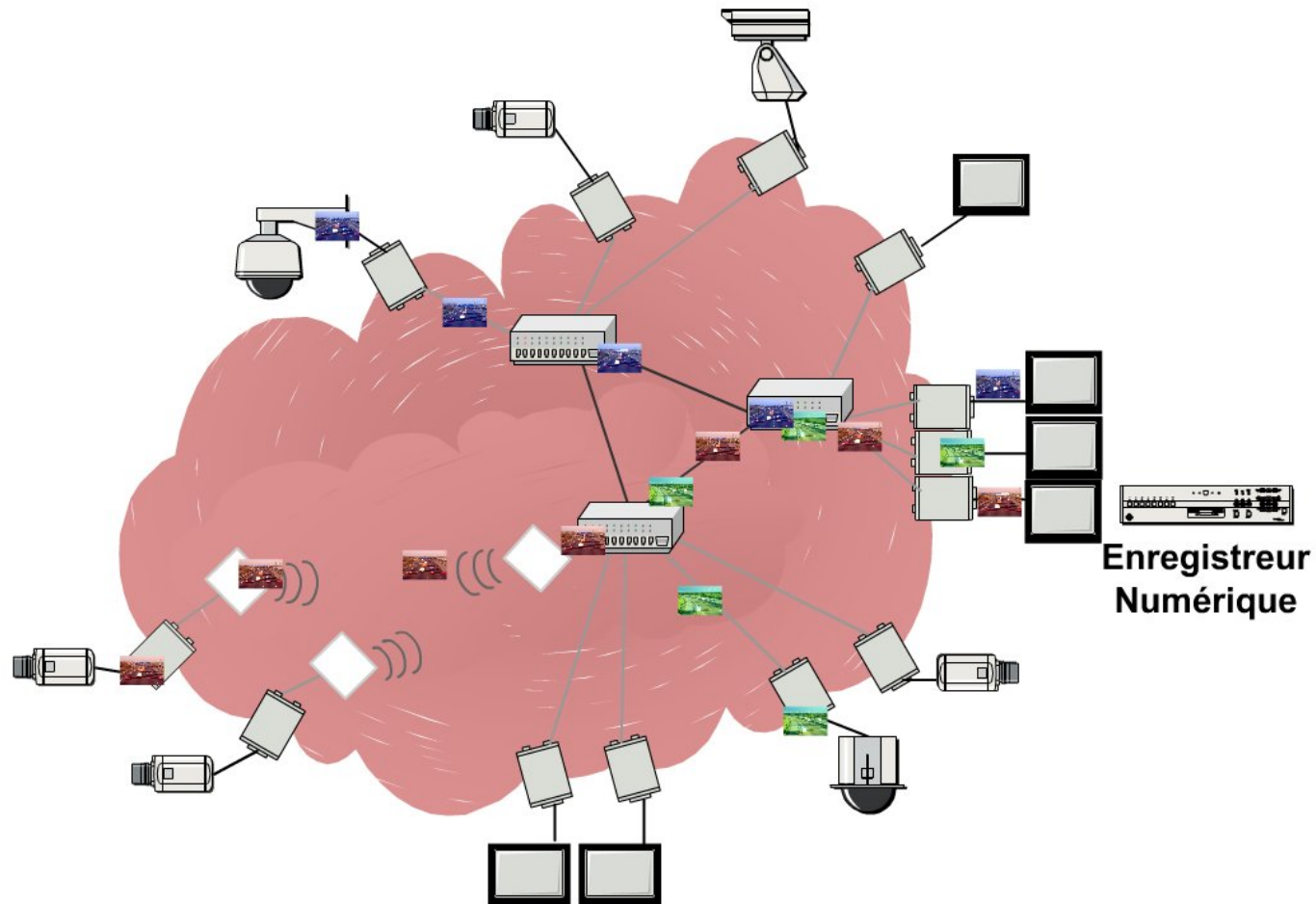
➔ **Cinq ans d'emprisonnement et de 300 000 € d'amende**

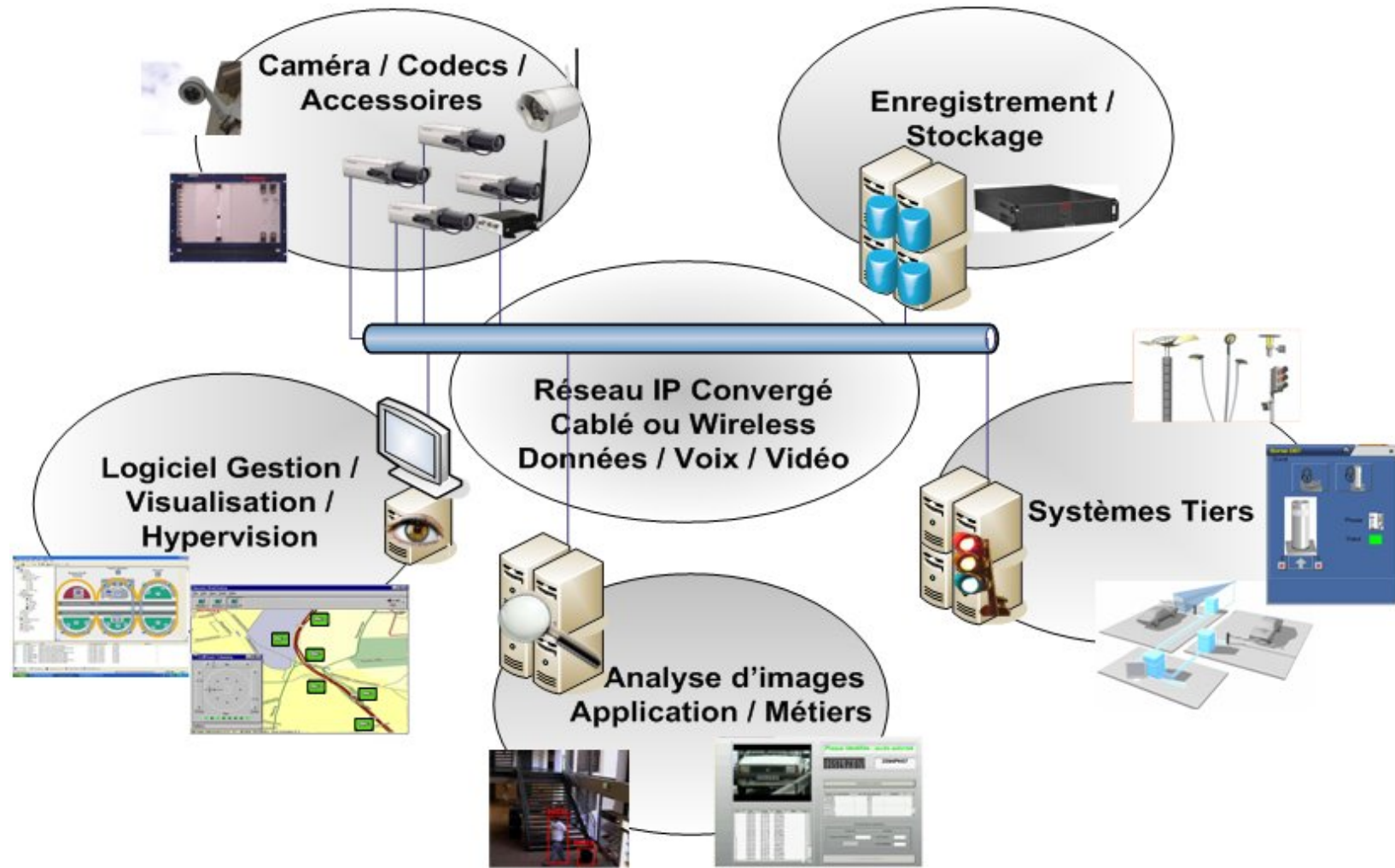
mardi 8 mars 2005 **Smart condamné pour vidéosurveillance**

Accusés par le comité d'entreprise, les dirigeants de l'usine d'automobiles Smart d'Hambach (Moselle) ont été condamnés lundi par le tribunal correctionnel de Sarreguemines pour la mise en place d'un système de vidéosurveillance à l'insu des salariés, notamment dans les toilettes.

02/08/06 **Vidéosurveillance: un pictogramme doit les signaler** Les systèmes de vidéosurveillance sur la voie publique doivent désormais être signalés par un pictogramme représentant une caméra. Ce signalement s'effectue par affiche ou panneau. C'est ce qu'indique un décret paru au Journal officiel du 28 juillet 2006.

02/06/06 **Condamnation définitive d'une société qui avait collecté des données personnelles sensibles** La CNIL avait, en 2002, dénoncé au parquet une société qui avait utilisé un sondage politique, présenté comme anonyme, pour recueillir des adresses électroniques et d'autres données personnelles. Le tribunal correctionnel de Nanterre avait condamné cette société, le 4 juin 2004, pour collecte déloyale et détournement de finalité d'un traitement informatique. Après le désistement du dirigeant de la société devant la Cour d'appel de Versailles, la condamnation est devenue définitive.





- **Fixer des normes techniques minimales**
  - pour les caméras
  - pour les systèmes de transmission
  - pour les systèmes de stockage
  
- **Fixer des normes d'interopérabilité**
  - pour les systèmes de stockage et d'export des données vers les forces de police (Mise à disposition des systèmes)

- La qualité des images restituées doit permettre d'atteindre les objectifs définis
  - contraintes sur les caméras
  - contraintes sur les réseaux
  - contraintes sur les systèmes de stockage
  - exigences sur la sécurité
- Les systèmes de stockage doivent être numériques, sauf pour les petites installations (moins de 8 caméras)
- Ils doivent garantir l'intégrité des images et des données associées (date, heure, id caméra, etc..)

- **Pour les caméras destinées principalement à l'identification des personnes :**
  - identification des personnes : Format 4 CIF (704 x 576) ou à défaut définition de visage de 90 X 60 pixels utiles au minimum
  - 6 images par seconde
  - sauf si déplacement des personnes : 12 images par seconde
  
- **les autres caméras**
  - format CIF (352 x 288) 6 images par seconde

Fixe des normes techniques sur les caméras et sur les systèmes de transmission et de stockage, d'exportation des données vers les forces de police et de gendarmerie

### → Recevabilité de la PREUVE

#### ■ **Caractéristiques techniques du système cohérentes avec les finalités**

- Qualité d'image, IPS, débit de transmission (codec),
- Caractéristiques d'authentification pour procédures judiciaires ; (DICP) pouvoir certifier la qualité de l'image et ses informations spatiales et temporelles.
- Conditions d'exportation ; Date heure durée de l'image id camera, date et heure export et identification personne, sur support non réinscriptible (logiciel de lecture sur support séparé)
- Exemple ;
- Caméra d'un terminal de paiement ; 4CIF, 6 IPS, plan étroit , (2 Mbs si JPEG)

*CIF* : 352 points (Horizontaux) sur 288 points (Verticaux).



**MERCI DE VOTRE ATTENTION**

*Jean-marc.chartres@telindus.fr*