Commission Nationale de l'Informatique et des Libertés

Communiqué de presse

21 juin 2012

Vidéosurveillance/vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée

Dans la rue, dans les magasins, les transports en commun, les bureaux, les immeubles d'habitation, difficile d'échapper aux 935 000 caméras installées en France. Depuis mars 2011, la CNIL est compétente pour contrôler l'ensemble de ces dispositifs sur le territoire national. Forte des constats opérés lors des contrôles réalisés en 2011, elle souhaite aujourd'hui accompagner les professionnels et les particuliers dans une démarche de conformité. Elle leur propose donc des bonnes pratiques pour que les dispositifs installés soient respectueux du cadre légal et des droits des personnes filmées. Elle s'associe notamment à l'AMF (Association des Maires de France) pour des recommandations spécifiques à destination des maires.

Dès que l'on sort de chez soi, on peut être filmé dans le hall de son immeuble, puis dans la rue sur le chemin du bus pour se rendre à son travail. Des caméras peuvent également être présentes dans les transports en commun. A son arrivée sur son lieu de travail, on peut aussi être filmé par les caméras installées par l'employeur.

Lors de la pause déjeuner, le magasin où l'on achète sa salade, ou celui où l'on fait ses courses, possède également des caméras pour éviter les vols. Retour au travail pour l'après-midi où une caméra est située dans le hall d'entrée de la société…

Le soir, même chemin pour rentrer chez soi, avec des arrêts au distributeur automatique pour retirer de l'argent, sous l'œil d'une caméra, et à la boulangerie pour acheter son pain avec une caméra surveillant la caisse.

On compte **897 750 caméras autorisées depuis 1995**, dont 70 003 pour la voie publique et 827 749 pour les lieux ouverts au public (commerces par exemple)*. La CNIL a quant à elle reçu **35 000 déclarations de dispositifs de vidéosurveillance depuis 1978** (pouvant être constitués de une à plusieurs dizaines de caméras). Ceux-ci concernent principalement la vidéosurveillance au travail.

Quel cadre légal ?

L'installation de ces outils est soumise au respect de plusieurs dispositions légales, selon qu'elles sont mises en place dans un lieu ouvert ou non au public.

Les dispositifs de vidéoprotection installés sur la voie publique et dans les lieux ouverts au public sont soumis aux dispositions du code de la sécurité intérieure. Depuis la loi du 14 mars 2011, dite LOPPSI 2, on ne parle en effet plus de vidéosurveillance mais de vidéoprotection. Ces dispositifs doivent obtenir une autorisation préfectorale, après avis d'une commission départementale présidée par un magistrat.

**chiffres issus du rapport 2011 du Ministère de l'intérieur relatif à l'activité des commissions départementales*

Les dispositifs de vidéosurveillance installés dans les lieux non ouverts au public (bureaux d'une entreprise, immeubles d'habitation) sont quant à eux soumis aux dispositions de la loi du 6 janvier 1978 modifiée, dite « Informatique et Libertés ». A ce titre, ils font l'objet d'une déclaration à la CNIL.

Quel contrôle ?

La CNIL contrôlait jusqu'alors les seuls dispositifs de vidéosurveillance. Depuis la LOPPSI 2, la CNIL dispose de pouvoirs lui permettant de contrôler également les dispositifs de vidéoprotection afin de s'assurer qu'ils sont conformes aux obligations légales. La CNIL peut procéder à ces contrôles de sa propre initiative ou à la demande de la commission départementale de vidéoprotection. Le responsable d'un dispositif de vidéoprotection peut aussi demander à la CNIL de vérifier la légalité des caméras qu'il a installées. Le contrôle mené par la CNIL consiste en une visite sur place.

La CNIL a reçu en 2011 plus de 360 plaintes relatives à la vidéoprotection et la vidéosurveillance, ce qui représente une augmentation de 32% par rapport à 2010. 60% de ces plaintes (soit 215 plaintes) concernaient la vidéosurveillance au travail (+ 13% par rapport à 2010).

La CNIL a procédé à **150 contrôles de dispositifs de vidéoprotection en 2011 et déjà 80 en 2012**. A cette occasion elle a constaté :

- une nécessaire clarification du régime juridique ;
- une information des personnes insuffisante ou inexistante ;
- une mauvaise orientation des caméras ;
- des mesures de sécurité insuffisantes.

Quelles bonnes pratiques pour concilier sécurité collective et respect de la vie privée ?

Forte de ces constats, la CNIL souhaite aujourd'hui accompagner les professionnels et les particuliers. C'est pourquoi elle met à leur disposition des fiches pratiques leur expliquant concrètement comment installer des dispositifs dans le respect de la loi et du droit des personnes filmées. Le site de la CNIL propose 6 fiches pratiques :

- La vidéoprotection sur la voie publique
- La vidéosurveillance au travail
- La vidéosurveillance dans les établissements scolaires
- Les caméras dans les commerces
- La vidéosurveillance dans les immeubles d'habitation
- La vidéosurveillance chez soi

Enfin, la CNIL et l'AMF (Association des Maires de France) ont élaboré conjointement des bonnes pratiques à destination des maires qui souhaitent installer des systèmes de vidéoprotection dans le respect des libertés individuelles. Ces 10 conseils sont disponibles sur les sites de l'AMF et de la CNIL. Cette initiative commune s'inscrit dans le cadre de la convention de partenariat signée entre les deux organismes le 15 juin 2011.

LES CONTROLES SUR LA VIDEOPROTECTION EFFECTUES PAR LA CNIL : BILAN ET PLAN D'ACTION

La loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 (LOPPSI 2) a notamment modifié l'article 10 de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, afin de permettre à la CNIL de contrôler les dispositifs dits « de vidéoprotection ». La compétence de la Commission est donc désormais expressément reconnue pour le contrôle tant des dispositifs de vidéoprotection soumis aux articles L.251-1 et suivants du code de la sécurité intérieure (pour la voie publique et les lieux ouverts au public) que pour les dispositifs de « vidéosurveillance » soumis à la loi de 1978 (pour les lieux non accessibles au public telles que les zones réservées au salariés).

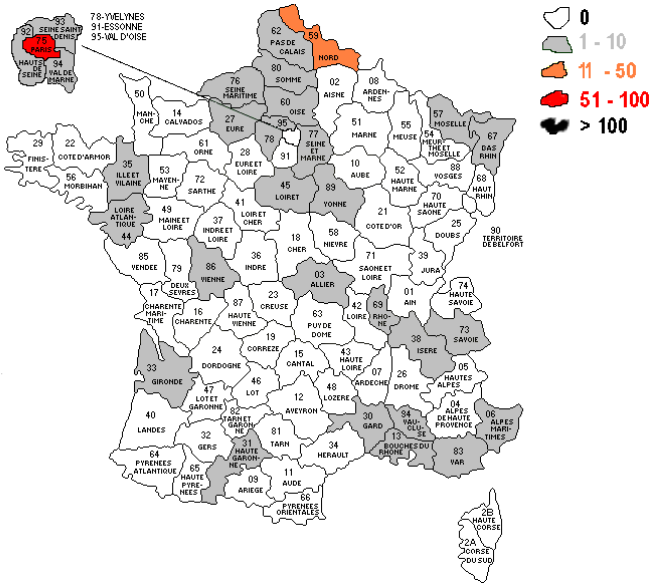
> *« La Commission nationale de l'informatique et des libertés peut, sur demande de la commission départementale prévue au premier alinéa du présent III, du responsable d'un système ou de sa propre initiative, exercer un contrôle visant à s'assurer que le système est utilisé conformément à* [l'autorisation préfectorale le concernant] *et, selon le régime juridique dont le système relève, aux dispositions de la présente loi ou à celles de la loi n° 78-17 du 6 janvier 1978 précitée* »[1].
>
> **LOPPSI 2, 14 mars 2011**

Quelle méthodologie ?

La CNIL a immédiatement utilisé cette nouvelle compétence puisqu'elle a effectué plus de 150 contrôles au cours de l'année 2011.

Cet effort sera prolongé au cours de l'année 2012 puisque la CNIL s'est fixée comme objectif de réaliser, au cours de l'année 2012, 150 contrôles portant sur les dispositifs de vidéoprotection. 80 d'entre eux ont déjà été réalisés.

Ainsi, au total, depuis l'adoption de la loi de mars 2011, la CNIL a réalisé plus de **230 contrôles** portant sur des dispositifs de vidéoprotection.



Carte des contrôles des dispositifs de vidéoprotection réalisés depuis mars 2011

Ces contrôles ont été réalisés à **75% auprès du secteur privé** (magasins, hôtels, restaurants, entreprises, banques, etc.) et à **25% auprès du secteur public** (gares, écoles, musées, collectivités locales, etc.).

Les organismes contrôlés ont été choisis afin de s'assurer de l'application de la loi dans l'ensemble des situations où un système vidéo peut être déployé. Ainsi, les organismes contrôlés ont été identifiés en fonction de leur taille – et donc du nombre de personnes filmées - (par exemple, des contrôles ont été diligentés dans des commerce de petite taille et dans des grands magasins parisiens), de leur localisation (centres commerciaux et centres villes) et, également, parfois, en fonction de l'actualité (article de presse soulignant la mise en œuvre d'un dispositif).

Les principaux points vérifiés par la CNIL sont les suivants :

- le respect de l'autorisation préfectorale délivrée quant à la finalité du dispositif et l'orientation des caméras ;
- le masquage des zones privées (maisons, appartements, etc.) ;
- la durée de conservation des images ;
- l'information des personnes filmées ;
- les mesures de sécurité entourant le dispositif.

Environ **15% des contrôles** ont été effectués dans le cadre de l'instruction de plaintes.

On doit en effet rappeler que le code de la sécurité intérieure prévoit expressément que « *Toute personne intéressée peut saisir* […] *la Commission nationale de l'informatique et des libertés de toute difficulté tenant au fonctionnement d'un système de vidéoprotection* ». Ainsi, la CNIL a, par exemple, été saisie par des salariés s'interrogeant sur la légalité de caméras placées dans leur entreprise ou encore de clients ayant remarqué un dispositif de vidéoprotection en l'absence d'information à destination du public, etc.

La CNIL a été saisie de demandes de la SNCF et de la RATP souhaitant que des contrôles soient réalisés afin de vérifier la conformité de leurs dispositifs de vidéoprotection. Le code de la sécurité intérieure (article L. 253-2) permet en effet à un responsable d'un système de vidéoprotection de saisir la CNIL afin que celle-ci effectue un contrôle sur ses installations. La CNIL a effectué plus d'une trentaine de contrôles dans des gares situées à Paris et en province, et dans certaines stations de métro.

Ces contrôles ont démontré une application satisfaisante de la loi et vont permettre la rédaction, en collaboration avec la CNIL, de chartes visant à encadrer le développement de ces systèmes dans le respect de la vie privée des personnes concernées.

Quels constats ?

- **Les responsables contrôlés ont parfaitement identifié la compétence de la CNIL** en matière de contrôle des systèmes de vidéoprotection.

Les contrôles ont permis de constater qu'aucun des dispositifs vérifiés par la Commission – à l'exception d'un seul – n'avait fait l'objet d'un contrôle de la part d'une autre autorité (forces

de police, préfectures, etc.). L'activité de la CNIL remplit donc bien un « vide » en termes de contrôle de dispositifs potentiellement intrusifs pour la vie privée des personnes.

- Environ **50% des dispositifs contrôlés relèvent à la fois du code de la sécurité intérieure** (caméras filmant des zones ouvertes au public : espace « clients ») **et de la loi « Informatique et Libertés »** (zones non ouvertes au public : espace « réservés » aux salariés).

L'existence d'un double régime juridique pour un même système selon les zones filmées peut donc conduire les responsables concernés à s'interroger sur leurs obligations légales.

C'est pourquoi la CNIL a entamé une démarche de pédagogie afin d'informer et de sensibiliser les responsables aux exigences légales en matière d'installation de caméras.

- **Un manque d'homogénéité dans les autorisations délivrées par les différentes préfectures a été constaté,** que ce soit concernant leur compétence (application ou non du code de la sécurité intérieure à des lieux tels que des crèches ou des espaces non ouverts au public dans des maisons de retraite) ou quant aux zones pouvant être filmées (par exemple, certaines préfectures refusent que les zones où se restaurent les personnes soient filmées, d'autres l'acceptent).

Enfin, les contrôles ont permis de constater d'une part, l'utilisation de caméras factices et, d'autre part, des dysfonctionnements pouvant affecter les dispositifs vidéo (absence d'enregistrement, mauvaise qualité de l'image, etc.).

Quels manquements ?

Les **principaux manquements** concernant les conditions de mise en œuvre effective des dispositifs vidéo, relevés à l'occasion des contrôles sont les suivants :

- Une absence d'autorisation ou absence de renouvellement préfectorale (environ 30% des contrôles). Les absences d'autorisation préfectorale sont le plus souvent des cas constatés lorsqu'un contrôle est effectué pour apprécier la régularité d'un dispositif soumis à la loi de 1978 et qu'il fait apparaître un dispositif filmant également des lieux ouverts au public ;
- Une absence de déclaration à la CNIL pour les parties de dispositifs relevant de la loi de 1978 (environ 60% des cas) ;
- Une information des personnes inexistante ou une insuffisance (environ 40% des contrôles) ;
- Une mauvaise orientation des caméras (environ 20% des contrôles). Certains contrôles ont permis de constater des caméras « cachées », par exemple dans les détecteurs de fumées ;
- Une absence de masquage qui peut permettre à certains systèmes de vidéoprotection de visualiser voire enregistrer des images relevant de parties privatives d'immeubles ;
- Une durée de conservation excessive (environ 10% des contrôles) ;
- Des mesures de sécurité insuffisantes (environ 20% des contrôles).

Quelles suites données a ces contrôles ?

La CNIL a ainsi adopté, depuis le début de l'année 2011, environ **une vingtaine de mises en demeure** dont trois concernant spécifiquement des dispositifs filmant la voie publique. Les préfectures territorialement compétentes en ont été informées.

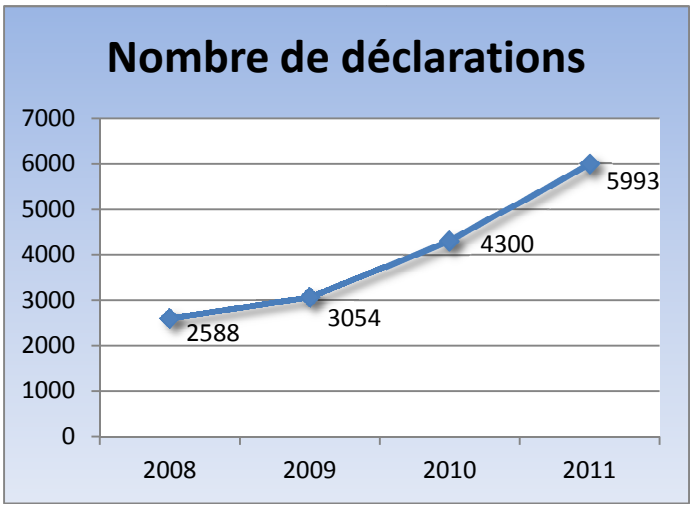
La CNIL a également prononcé en 2012, une sanction pécuniaire et un avertissement à l'encontre de responsables de systèmes de vidéosurveillance ne respectant pas les dispositions de la loi "Informatique et Libertés".

Quelles perspectives ?

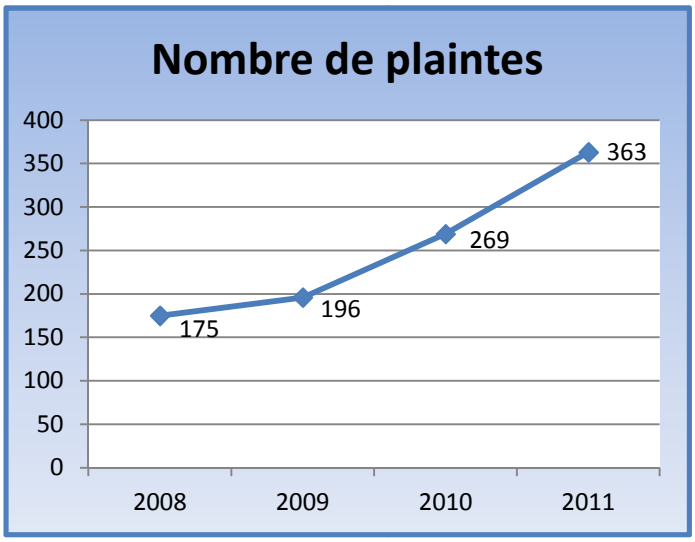
Les prochains mois seront notamment consacrés à la réalisation de contrôles des dispositifs de vidéoprotection qui concernent un nombre important de personnes (dispositifs mis en œuvre au sein des collectivités locales ou au sein de structures accueillant un nombre important de personnes), et les dispositifs dits de « vidéoverbalisation ». La CNIL assurera également la promotion des bonnes pratiques élaborées en collaboration avec l'AMF (Association des Maires de France) et des fiches pratiques sectorielles qu'elle a conçues et mis en ligne sur son site.

LES CHIFFRES DE LA VIDEO

La vidéosurveillance



+ 37% de déclarations par rapport à 2010 - 35 000 déclarations à la CNIL depuis 1978



+ 32 % de plaintes par rapport à 2010. En 2011, 60% de ces plaintes concernaient des dispositifs de vidéosurveillance sur les lieux de travail (+13% par rapport à 2010).

La vidéoprotection

- 897 750 caméras autorisées depuis 1995, dont 70 003 pour la voie publique et 827 749 pour les lieux ouverts au public (Chiffres issus du rapport 2011 relatif à l'activité des commissions départementales du Ministère de l'intérieur).
- 170 042 caméras installées en 2011 (+13% par rapport à 2010)
- 38 000 caméras surveillant la voie publique en fonctionnement
- 150 contrôles de la CNIL en 2011 et 80 en 2012

HISTOIRES VUES, HISTOIRES VECUES

- Madame B., déléguée syndicale, a adressé une plainte à la CNIL à la suite de l'installation de caméras dans son entreprise. Deux caméras filmaient la badgeuse ainsi que le couloir menant à la salle de pause et au local syndical. La CNIL a contacté l'employeur de Madame B pour lui rappeler que la vidéosurveillance ne doit pas être disproportionnée et ne peut pas filmer les locaux syndicaux. L'employeur a finalement décidé de changer l'orientation de la première caméra et a supprimé la deuxième.

- Lors d'un contrôle dans un supermarché, les services de l'Inspection du travail constatent la présence d'une caméra dissimulée dans un boîtier électrique de la réserve du magasin. Ils en avertissent la CNIL qui écrit à la société exploitant le supermarché pour lui rappeler que le fait d'installer une caméra à l'insu des personnes n'est pas légal. La société indique que cette caméra présente peu d'intérêt et accepte, à la demande de la CNIL, de la supprimer.

- Monsieur et Madame R., qui habitent dans le sud-ouest, constatent que le casino dont ils sont voisins, diffuse en direct sur son site internet des images de leur maison. Ces images proviennent des caméras installées sur le casino. Leur maison, de même que la voie publique sont visibles de tous, et ce, en permanence. Monsieur et Madame R. s'adressent à la CNIL. Celle-ci contacte le responsable du casino pour lui rappeler qu'il est excessif de filmer des lieux d'habitation sans l'autorisation des occupants et de diffuser ces images sur internet. De plus, les personnes morales de droit privé ne sont pas autorisées à filmer la voie publique en application du code de la sécurité intérieure. A la demande de la CNIL, le casino a finalement décidé de mettre hors service ces caméras dont l'objectif était de montrer les conditions climatiques en temps réel.

CE QU'IL NE FAUT PAS FAIRE !

- **Filmer la cour de recréation d'un établissement scolaire 24h/24**
- **Filmer la voie publique pour surveiller sa voiture garée devant chez soi**
- **Filmer l'intérieur d'appartements privés ou les portes des appartements au sein d'une copropriété**
- **Filmer en permanence le bureau d'un salarié**
- **Filmer les salles de pause dans une entreprise**
- **Filmer l'entrée du local syndical d'une entreprise**
- **Cacher des caméras pour filmer des salariés à leur insu**
- **Placer une caméra dans une chambre d'hôtel**
- **Filmer les vestiaires d'une piscine municipale ou d'une salle de sport**
- **Filmer les toilettes d'un restaurant ou d'une entreprise**
- **Enregistrer les images sans limitation de durée**

ZOOM SUR LA VIDEO DE DEMAIN

Au-delà du contrôle des systèmes en place, la CNIL cherche à anticiper les nouveaux usages et nouvelles technologies qui modifieront le besoin de régulation dans les années à venir. La vidéo et ses évolutions sont donc un axe de travail à la fois pour le laboratoire de la CNIL créé en 2011 et pour le programme d'études prospectives 2012-2013.

Quelles sont les tendances lourdes et émergentes les plus marquantes dans ce domaine ?

1. L'extension du domaine de la vidéo

La CNIL constate une tendance lourde à la **multiplication des finalités de surveillance** : contrôle du respect de la règlementation sur les déjections canines, contrôle des agents travaillant sur la voie publique (« vidéotranquillité »), systèmes de péages urbains sans barrières (par lecture automatisée des plaques d'immatriculation à Londres), vidéoverbalisation, etc.

Tout autant que les finalités, les plateformes porteuses de caméras vont se multiplier : projets de caméras portées par les agents de police afin de servir d'éléments de preuve en cas de problèmes liés à une intervention, usage de drones civils pour des prises de vue en mobilité.

La transmission des images par internet (déjà source de nombreuses plaintes auprès de la CNIL), risque également de s'accroitre dans les années à venir. Ce phénomène est dû à la généralisation rapide des smartphones permettant l'enregistrement de vidéo de qualité et leur publication instantanée, grâce au débit des réseaux mobiles (3G, …). Stockées en ligne de manière indéfinie, ces images pourraient être susceptibles de faire l'objet de traitement ultérieur avec des technologies nouvelles, par exemple des technologies de recherche dans les contenus par mots clés ou annotations, elles sont aussi en cours de développement[1].

Le marketing est une finalité de plus en plus courante. Les caméras installées dans des supermarchés permettent de mesurer la fréquentation d'un magasin et le parcours des clients. Des caméras sur des panneaux publicitaires comptent le nombre de personnes qui regardent le panneau, le temps passé devant celui-ci, et parfois même estiment l'âge et le sexe afin de mesurer précisément leur audience. Cet œil du marketing pourrait même être demain présent dans votre salon : certains modèles de téléviseurs de nouvelle génération (« smart TV ») sont équipés de caméras permettant le contrôle gestuel, la personnalisation de l'interface, voire demain la personnalisation des publicités ou une mesure d'audience en temps réel, avec une analyse de posture pour « qualifier » les réactions du téléspectateur.

2. Vers la vidéo « analytique » et prédictive

La tendance d'innovation la plus prégnante est l'intégration d'outils logiciels de remontée d'alerte automatiques, grâce par exemple à l'analyse de comportements.

[1] Par exemple dans le cadre du projet de R&D américain VIRAT (http://en.wikipedia.org/wiki/VIRAT)

Au premier niveau, il s'agit simplement d'automatiser et d'accompagner certaines tâches. Ainsi, un système proposé par un industriel français permet le suivi en temps réel de personnes afin de permettre une interception par un agent de sécurité d'une personne déterminée (par exemple une personne ayant pénétré dans un endroit interdit d'accès). Cette personne est ensuite suivie par caméras lors de ses déplacements tandis qu'une information est transmise à un agent afin que ce dernier arrive à sa rencontre. La technologie met en œuvre de la détection de contour et de la détection de la tenue vestimentaire, sans pour autant utiliser de technologies d'identification.

Mais au-delà de cette automatisation de tâches simples, certaines de ces fonctionnalités ont comme objectif **d'accroitre les prétentions prédictives** des systèmes de vidéosurveillance et vidéoprotection. Ainsi, une équipe de l'INRIA a d'ores et déjà réalisé un prototype fonctionnel en matière de détection de groupes et de comportements (voir image ci-contre). Ces systèmes sont particulièrement intéressants pour des missions de surveillance automatisée de foules, dans des lieux publics densément occupés comme des gares, centres commerciaux, ou encore des manifestations sur la voie publique.
Les systèmes de vidéosurveillance de ce type chercheront donc à détecter automatiquement ce qu'ils qualifient d'anomalies, d'« anormalités ».

3. Le couplage avec d'autres technologies : son, reconnaissance faciale

L'autre grande tendance est au couplage du flux vidéo issu des caméras avec d'autres informations issues de capteurs ou de fichiers.
La qualité croissante des images captées par les caméras disponibles sur le marché permet en effet d'envisager le lien avec des fichiers, par exemple d'images enregistrées par l'application d'une technologie de reconnaissance faciale. Cette technologie est d'ores et déjà utilisée sur des flux vidéo pour l'identification des personnes présentes sur des *watch list* dans des aéroports, des gares, des casinos ou des stades sportifs. La CNIL a ainsi autorisé en avril 2010 une expérimentation (projet « biorafale »[2]) concernant un traitement de reconnaissance faciale en temps réel dans un stade pour des personnes volontaires visant à repérer automatiquement les interdits de stade.

Mais, la logique de ce couplage vidéo/reconnaissance faciale s'étend bien au-delà de la confrontation des images à une simple *watch list* ou liste noire : **l'ambition est bien de confronter la vidéo à des grands volumes d'images issus de fichiers d'identification**. Le Livre blanc sur la sécurité publique remis au Ministre de l'intérieur en 2011 propose ainsi la création « d'une véritable base nationale de photographies » afin de « développer le recours aux logiciels de reconnaissance automatisée par l'image pour en faciliter l'exploitation et

[2] Projet expérimental proposé par la société VELSAIS, ayant pour objet la reconnaissance faciale de personnes en environnement non contraint.

accélérer la résolution des enquêtes judiciaires disposant d'indices tirés de la vidéoprotection »[3].

Certains testent également le couplage des systèmes de vidéosurveillance avec des microphones. Ce type de système est mis en place par exemple dans la commune de Birmingham en Angleterre. Ainsi, par triangulation des sons captés, il est possible de connaitre la position d'un coup de feu et ensuite de repérer plus facilement les personnes concernées par la fusillade. Ce type de système pose des problèmes nouveaux : en effet, si le son est enregistré, rien n'interdit techniquement d'enregistrer des conversations et pourquoi pas de les analyser pour remonter une alerte lorsque certains mots seraient cités.

[3] Proposition numéro 42.

GLOSSAIRE

Vidéosurveillance
Identifie un dispositif de caméras permettant de visionner des images dans un **lieu non ouvert au public**.

Vidéoprotection
Identifie un dispositif de caméras permettant de visionner des images sur la **voie publique** ou dans un **lieu ouvert au public** en conformité avec les dispositions du code de la sécurité intérieure.

Lieu ouvert au public
Un lieu ouvert au public est un lieu pour lequel il n'existe **pas de restriction d'accès**. Le simple paiement d'une somme d'argent n'est pas considéré comme constituant une restriction d'accès. Ainsi, les commerces, les boîtes de nuit, les cinémas, les restaurants, les services publics recevant les usagers, les parcs d'attraction sont considérés comme des lieux ouverts au public.

Lieu non ouvert au public
Constitue un lieu non ouvert au public celui pour lequel il existe une **restriction d'accès.** Le simple paiement d'une somme d'argent n'est pas considéré comme constituant une restriction d'accès. Ainsi, les bureaux d'un organisme public ou privé, les réserves et autres lieux dédiés au personnel, les établissements scolaires, les parties communes d'immeubles d'habitation (lorsqu'elles sont accessibles avec un interphone, un digicode ou une clé) sont des lieux non ouverts au public.

Autorisation préfectorale
Arrêté pris par le préfet du département autorisant la mise en place d'un dispositif de vidéoprotection sur la **voie publique** ou dans un **lieu ouvert au public**.

Déclaration
Formalité à accomplir sur le site internet de la CNIL par toute personne privée ou publique souhaitant installer un dispositif de vidéosurveillance dans un **lieu non ouvert au public**.

Traitement de données à caractère personnel
Un dispositif manuel ou informatisé comportant des données permettant d'identifier directement ou indirectement une personne physique.

Correspondant informatique et libertés
Personne désignée par le responsable d'un traitement de données personnelles afin de l'aider à se conformer aux règles relatives à la protection des données personnelles.

LES CAMERAS : AUTORISEES OU DECLAREES ?

Ce tableau résume les différentes formalités administratives qui doivent être accomplies en France avant d'installer des caméras dans un lieu ouvert ou non au public.

LIEU D'INSTALLATION	AUTORISATION PREFECTORALE	DECLARATION A LA CNIL
Voie publique (rue)	●	
Lieux ouverts au public (commerces, banques, administrations, aéroports, gares, etc.)	●	
Lieux non ouverts au public dans les commerces, administration, etc. (réserves, zones réservées au personnel, etc.)		●
Etablissements scolaires (abords)	●	
Etablissements scolaires (intérieur)		●
Lieux communs ouverts au public dans un immeuble d'habitation	●	
Lieux communs non ouverts au public dans un immeuble d'habitation		●
Domicile personnel		
Domicile personnel avec des salariés		●