

L'IMPACT DE LA LOI INFORMATIQUE ET LIBERTÉS SUR LES TRAITEMENTS ET FICHIERS DANS LA RELATION DE TRAVAIL : APPROCHE DE LA CNIL

Laurent LIM

Attaché à la Direction juridique

CNIL

ALLIANCE TICS – Commission juridique

28 Septembre 2006

RÉFORME DU 6 AOÛT 2004 : LES POINTS CLÉS DE LA NOUVELLE LOI INFORMATIQUE ET LIBERTÉS

- les grands principes inchangés mais un renforcement des droits des personnes
- une redéfinition des missions de la CNIL:
l'allègement des formalités déclaratives
- de nouveaux pouvoirs de sanctions pour la CNIL
- l'institution des correspondants à la protection des données

LA CNIL : STATUT ET COMPOSITION INCHANGÉS

- une autorité administrative indépendante composée de 11 membres (hauts magistrats, parlementaires, conseillers économiques et sociaux, personnalités qualifiées)
- un président élu par ses pairs: M. Alex Türk, sénateur du Nord.
- l'absence de contrôle financier préalable des dépenses
- l'établissement de son règlement intérieur
- les membres de la CNIL ne reçoivent d'instruction d'aucune autorité.
- budget: de l'ordre de 9 millions d'euros, services: 85 personnes.
- le nécessaire renforcement des moyens pour faire face à ses nouvelles missions

NOUVELLES MISSIONS ET POUVOIRS DE CONTRÔLE RENFORCÉS

- Un contrôle allégé sur la création des fichiers
- Mais un renforcement des pouvoirs de contrôle sur place et sur pièces
- Mais de nouveaux pouvoirs de sanctions administratives et pécuniaires
- Et une mission de conseil et d'information élargie: avis sur la conformité à la loi des projets de règles professionnelles et sur les produits tendant à la protection des données ou à l'anonymisation des données; délivrance de labels .

UN CONTRÔLE ALLÉGÉ SUR LA CRÉATION DES FICHIERS

- des fichiers **exonérés** de déclaration:
 - par la loi (ex; traitements pour des activités personnelles, fichiers de membres de partis politiques, d'églises, de syndicats...)
 - par la CNIL (ex: **fichiers de paie**, de fournisseurs, dématérialisation des marchés publics, blogs...)
 - sous certaines conditions, par la **désignation de correspondants à la protection des données**

UN CONTRÔLE ALLÉGÉ SUR LA CRÉATION DES FICHIERS

- **La déclaration devient le régime de droit commun (art 22 et 23):**
 - un dossier de déclaration allégé (formulaire et annexes) disponible sur www.cnil.fr; la télédéclaration pour les sites web;
 - **Les cabinets d'avocats doivent déclarer leurs fichiers de clients sauf s'ils désignent un correspondant.**
- **La CNIL peut adopter des mesures de simplification: les normes simplifiées (70% des traitements déclarés).**
 - une procédure de télédéclaration sur www.cnil.fr ;
 - 50 normes simplifiées (ns) : ex: la ns 46 pour les fichiers de gestion du personnel, la ns 42 pour les contrôles d'accès et d'horaires, la ns 47 pour les dépenses téléphoniques...

...MAIS UN CONTRÔLE PRÉALABLE RENFORCÉ SUR LES TRAITEMENTS DE DONNÉES PRÉSENTANT DES RISQUES PARTICULIERS (AVIS OU AUTORISATION)

- **Un régime d'avis préalable motivé et publié de la CNIL (art 26 et 27)** par exemple pour les traitements de l'État intéressant la sûreté, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté; pour les téléservices de l'administration électronique...
- **Une autorisation de la CNIL pour 10 catégories de traitements (art 25):** par exemple pour les traitements de données biométriques (ex; pour des contrôles d'accès ou d'horaires), les traitements qui comportent des appréciations sur les difficultés sociales des personnes (ex: fichiers de gestion de l'action sociale) ;les traitements de données génétiques;portant sur les infractions, condamnations ou mesures de sûreté; (ex: sociétés de droit d'auteur), les interconnexions de fichiers différents, les traitements susceptibles d'exclure les personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence d'un cadre légal (ex credit scoring)

UN RENFORCEMENT DES POUVOIRS DE CONTRÔLE SUR PLACE (ART 44)

- accès à tous locaux professionnels;
- possibilité de demander tous documents nécessaires et d'en prendre copie, d'accéder aux programmes informatiques et aux données et d'en demander la transcription;
- mais seul un médecin peut requérir la communication de données médicales individuelles;
- les fichiers intéressant la sûreté de l'Etat peuvent, sous certaines conditions, échapper à ce contrôle.

DE NOUVEAUX POUVOIRS DE SANCTION (ART 45)

- la CNIL peut adresser des avertissements et des mises en demeure de faire cesser un manquement à la loi;
- elle peut ensuite prononcer des sanctions pécuniaires (sauf pour les traitements de l'Etat): jusqu'à 150 000 € et en cas de réitération, 300 000 € (ou 5 % du CA HT pour les entreprises dans cette limite);
- elle peut prononcer une injonction de cesser le traitement ou un retrait de l'autorisation et en cas d'urgence, décider l'interruption du traitement, le verrouillage des données, pour trois mois; en cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander, par référé, à la juridiction compétente, d'ordonner toute mesure de sécurité nécessaire;
- la CNIL a la possibilité de dénoncer au parquet les infractions à la loi dont elle a connaissance; sanctions pénales lourdes (art 226-16 et s du Code Pénal: de l'ordre de 5 ans d'emprisonnement, 300 000 euros d'amende).

LA CNIL: QUEL BILAN POUR 2005 ?

- **Le contrôle sur la création des fichiers**
 - plus d'1 million de fichiers déclarés à la CNIL depuis 1978
 - 84 000 déclarations en 2005 – 21 refus d'autorisation (biométrie, crédit scoring, lutte contre le peer to peer- geolocalisation de véhicules...)
- **le développement des missions de contrôle sur place et sur pièces**
 - en 2005: près de 100 missions réalisées (banques, organismes de crédit, hôtels, grands magasins, collectivités locales...)
- **Le recours aux nouveaux pouvoirs de sanctions administratives et pécuniaires**
 - près de 3900 plaintes reçues en 2005 (+ 6 %) notamment dans les secteurs banques, crédit, fichiers centraux d'impayés, internet, marketing commercial
 - 50 dossiers examinés en formation de sanction: **36 mises en demeure, 10 avertissements** rendus publics (dans le secteur banques-crédit) pour des manquements concernant une utilisation incorrecte des fichiers d'incidents de paiement, absence de déclaration, créations de listes noires, non respect du droit de radiation des fichiers commerciaux, collecte déloyale, zones commentaires, non-respect du droit d'accès...
 - 3 dénonciations au parquet en 2004-2005.

EXEMPLES D'INTERVENTION DE LA CNIL

La régulation par :

- l'élaboration de normes juridiques : recommandations, normes
- le traitement des plaintes et des saisines
- la conduite de contrôles sur place
- la participation à des actions de formation et de communication

LES PROCEDURES DECLARATIVES

- Les dispenses de déclaration
- L'engagement de conformité :
 - à une norme simplifiée
 - à une autorisation
- La déclaration normale (modalités de « déclaration unique » possibles pour les groupes de sociétés)
- La demande d'autorisation pour les traitements les plus sensibles
- Les procédures de demandes d'avis

LES TRAITEMENTS AUTOMATISES DANS LE CADRE DE LA RELATION DE TRAVAIL

FINALITE	FORMALITES	CONDITIONS
<p>Paie (frais professionnels...)</p> <p>Déclarations obligatoires (DADS, DOETH, DPAE, déclarations AT)</p> <p>Tenue des registres obligatoires (RUP)</p> <p>Tenue des comptes individuels d'intéressement et participation</p> <p>Statistiques non nominatives</p>	AUCUNE	<p>Dispense n°2 (employeurs privés)</p> <p>Exclusion des transferts de données vers un pays tiers à l'Union Européenne</p>
Comptabilité générale	AUCUNE	Délibération n°80-34 du 21 octobre 1980
<p>Gestion des contrôles d'accès</p> <p>Gestion des horaires</p> <p>Gestion de la restauration d'entreprise</p>	<p>DECLARATION SIMPLIFIEE</p> <p>(Si correspondant désigné : AUCUNE)</p>	<p>NS 42</p> <p>Exclusion des traitements biométriques</p>

LES TRAITEMENTS AUTOMATISES DANS LE CADRE DE LA RELATION DE TRAVAIL

FINALITE	FORMALITES	CONDITIONS
<p>Fichiers courants de GRH : Gestion administrative (dossiers professionnels, annuaires internes, listes électorales, convocations)</p> <p>Mise à disposition d'outils informatiques (suivi, maintenance, annuaires informatiques, messageries, Internet)</p> <p>Organisation du travail (agendas professionnels, gestion des tâches)</p> <p>Gestion des carrières (évaluation, validation des acquis, mobilité...)</p> <p>Gestion de la formation</p>	<p>DECLARATION SIMPLIFIEE (Si correspondant désigné : AUCUNE)</p>	<p>NS 46</p> <p>Transferts de données vers un pays tiers à l'Union européenne possibles</p> <p>Exclusions :</p> <ul style="list-style-type: none">-traitements permettant le contrôle individuel de l'activité des employés-Dispositifs permettant l'établissement d'un profil psychologique (exclusion des traitements de recrutement) <p>Cf. recommandation recrutement du 21 mars 2002</p>

LES TRAITEMENTS AUTOMATISES DANS LE CADRE DE LA RELATION DE TRAVAIL

FINALITE	FORMALITES	CONDITIONS
<p>Mise en œuvre de services de téléphonie fixe et mobile sur les lieux de travail</p> <p>Gestion des communications (annuaire téléphoniques interne, gestion des dotations, messagerie téléphonique interne, maîtrise des dépenses liées à l'utilisation des services de téléphonie)</p>	<p>DECLARATION SIMPLIFIEE (Si correspondant désigné : AUCUNE)</p>	<p>NS 47</p> <p>Exclusions :</p> <ul style="list-style-type: none">- Ecoutes et enregistrements d'appels téléphoniques- Localisation d'un employé à partir d'un téléphone portable
<p>Alerte professionnelle</p>	<p>AUTORISATION</p>	<p>Autorisation n°4</p>
<p>Dispositifs biométriques</p>	<p>AUTORISATION</p>	<p>Autorisations n°7 et 8</p>

LES TRAITEMENTS AUTOMATISES DANS LE CADRE DE LA RELATION DE TRAVAIL

FINALITE	FORMALITES	CONDITIONS
<p>Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la CNIL, notamment :</p> <ul style="list-style-type: none">-traitements de contrôle de l'activité professionnelle (vidéosurveillance, surveillance des connexions internet, messageries)-traitements de recrutement (Bases de CV ou de candidats)-Fichiers médicaux gérés par la médecine du travail-Fichiers des CE de gestion des œuvres sociales-Transferts de données hors UE	<p>DECLARATION NORMALE (Si correspondant désigné : AUCUNE)</p>	<p>Déclaration normale (formulaire téléchargeable sur www.cnil.fr)</p>

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

**Dispositif d'alertes
professionnelle:**

**Les recommandations de
la CNIL et du groupe de
l'article 29**

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

- **UN CHAMP LIMITÉ** (pour l'autorisation unique)
Compte tenu du caractère complémentaire de ces dispositifs
- Domaines comptable, d'audit financier, de lutte contre la corruption ou bancaire : des faits se rapportant à des risques sérieux pour l'entreprise
- Une soupape de sécurité : faits graves car mettant en jeu l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés
Exemples : harcèlement moral, harcèlement sexuel, discriminations, délit d'initié, conflit d'intérêts, atteinte grave à l'environnement ou à la santé publique, mise en danger d'un autre employé, divulgation d'un secret de fabrique
- Quand il y a une obligation légale de communiquer l'information à un organisme public ou à une autorité compétente pour mener des poursuites pénales

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

- **LE TRAITEMENT DES ALERTES HORS DU CHAMP**
- **Faits particulièrement graves :**
Peuvent être recueillis et éventuellement réorientés vers les personnes compétentes au sein de l'entreprise
- **Alertes sur des faits qui ne sont pas graves et hors du champ :**
Réorienter l'émetteur vers le service compétent

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

- **LES CATÉGORIES DE PERSONNES CONCERNÉES : DÉFINITION PAR LE RESPONSABLE DU DISPOSITIF**
- Qui peut utiliser le dispositif d'alerte ?
Définition par l'employeur selon le principe de proportionnalité
En pratique : tous les employés
(/clients, fournisseurs)
- Qui peut faire l'objet d'une alerte ?
Même règle

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

IDENTIFICATION VERSUS ANONYMAT

L'émetteur de l'alerte professionnelle doit s'identifier :

- Intérêt de l'employeur (déroulement de l'enquête, climat de suspicion)
- Intérêt de l'émetteur (protection, enquête tournée vers l'émetteur)

mais son identité est traitée de façon confidentielle (communiquée ni à la personne

mise en cause, ni à sa hiérarchie – sauf nécessité liée à l'enquête-)

Si l'émetteur veut rester anonyme, son alerte est traitée sérieusement mais avec des précautions particulières (examen préalable, étiquetage « anonyme », anonymisation)

Quelles informations sur la possibilité d'utiliser le système anonymement ?

Pas de promotion ou d'encouragement

- Ne pas afficher au moment de la prise de contact téléphonique
- Mentionner dans l'information collective

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

LA NÉCESSITÉ D'UNE INFORMATION COLLECTIVE SUR LE DISPOSITIF

Une information générale en direction des utilisateurs potentiels

- Contenu :
 - Champ du dispositif
 - Identité du responsable, finalités, destinataires des données, droits des personnes, transfert de données hors Union européenne le cas échéant, existence et nom du prestataire extérieur
 - Risques encourus en cas d'utilisation abusive du dispositif
 - Absence de risque disciplinaire
 - Confidentialité de l'identité de l'émetteur
 - Avantages de l'identification
 - Précautions applicables au traitement d'alertes anonymes

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

UNE ORGANISATION DÉDIÉE AU TRAITEMENT DES ALERTES

- Une équipe de professionnels au sein de l'entreprise

Obligation renforcée de confidentialité (/obligation générale de confidentialité)

→ Un partage limité de l'information (supérieur, collègues)

- La possibilité d'une organisation spécifique à l'échelle du groupe

La communication de données légitimes si nécessaire à la vérification de l'alerte ou résulte de l'organisation du groupe

Condition : application des règles sur les transferts de données (contrats, Safe Harbor)

- La possibilité du recours à un prestataire extérieur

Condition : le prestataire s'engage par contrat à respecter les règles françaises et européennes de protection des données y compris les règles spécifiques (champ restreint, anonymat...)

Conclusion : la souplesse des mode d'organisation

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

L'INFORMATION DE LA PERSONNE FAISANT L'OBJET DE L'ALERTE

En principe dès l'enregistrement de données la concernant afin de lui permettre de s'opposer au traitement de ces données

- Après les mesures conservatoires nécessaires à la préservation des preuves
- Alerte hors du champ :
 - Si transmise à une personne compétente de l'entreprise compte tenu de sa gravité, information par le destinataire
 - Si archivée, information par le service « alertes »
 - Si détruite, aucune information

Contenu de l'information : entité responsable, les faits reprochés, destinataires de l'alerte, modalités d'exercice des droits d'accès et de rectification

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

CONSERVATION DES DONNÉES : DES DURÉES LIMITÉES

- Si alerte hors du champ : destruction ou archivage sans délai
- Conservation dans le système d'alerte :
Deux mois, à compter de la fin des opérations de vérification
À l'issue de cette période :
 - soit jusqu'à la fin de la procédure disciplinaire ou judiciaire
 - soit destruction ou archivage
- Archivage en dehors du système (accès restreint) : 30 ans
 - pour défendre les intérêts de l'entreprise en justice
 - à la demande de tiers autorisés
 - à la demande des personnes concernées exerçant leur droit d'accès

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

DROIT D'ACCÈS, DE RECTIFICATION ET D'OPPOSITION

- Droit d'avoir communication des données, sauf identité de l'émetteur de l'alerte et informations recueillies par enquête (documents préparatoires)
- Droit de demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la rectification ou la suppression

Exemples :

- Personne mise en cause de manière erronée → suppression
- Personne mise en cause de manière justifiée mais les données comportent des erreurs → rectification
- Droit de s'opposer... pour des motifs légitimes

Exemples :

- Absence d'information sur l'existence du dispositif, défaut manifeste de confidentialité

LES DISPOSITIFS D'ALERTE PROFESSIONNELLE

DOCUMENTS UTILES

- Autorisation unique n°4 (délibération du 8 décembre 2005) – en annexe : document d'orientation du 10 novembre 2005
- FAQ : www.cnil.fr (dossier Travail , rubrique Alertes professionnelles)
- Document du G 29 du 1er février 2006

LE CORRESPONDANT « INFORMATIQUE ET LIBERTÉS »: POURQUOI DÉSIGNER UN CORRESPONDANT ?

(art 22 loi 1978- art 42 et s du décret du 20.10.2005)

- permet de **dispenser de déclaration** la plupart des traitements (à l'exception des traitements à risque)
- assure, localement et de façon indépendante, **une meilleure application de la loi** et ainsi diffuse la culture informatique et libertés au sein de l'entreprise, de l'administration, de l'association...
- permet de disposer de **relations privilégiées avec la CNIL**: service dédié, délais de réponse plus rapides, information ciblée et adaptée

LE CORRESPONDANT « INFORMATIQUE ET LIBERTÉS »: QUELLES SONT SES MISSIONS ?

- le correspondant doit tenir la liste des traitements et la tenir à disposition de toute personne qui en fait la demande;
- **Il est chargé d'assurer d'une manière indépendante, le respect des obligations prévues dans la loi:** information, conseil, médiation, réception des plaintes, préparation de dossiers de formalités pour les traitements à risque, audits...
- il peut saisir la CNIL en cas de difficultés;
- en cas de manquement constaté à ses devoirs, il peut être déchargé de ses fonctions sur demande ou après consultation de la CNIL et en cas de non-respect de la loi, le responsable du traitement peut être enjoint de procéder aux formalités déclaratives.

LE CORRESPONDANT « INFORMATIQUE ET LIBERTÉS »:

QUI PEUT EXERCER CETTE FONCTION ?

- **Le correspondant ne peut être le responsable du traitement**
- **le responsable du traitement peut-il désigner un correspondant extérieur à l'organisme?**
 - oui mais sous certaines conditions pour les entités où plus de **50 personnes** sont chargées de la mise en œuvre des traitements ou y ont directement accès le correspondant ne peut être qu'un salarié du groupe de sociétés ou du GIE auquel appartient le responsable de traitements ou une personne mandatée par l'organisme professionnel ou regroupant des professionnels d'un secteur d'activité auquel appartient le responsable de traitement (ex : syndicat professionnel, chambre de commerce...)
- **quelles sont les qualifications requises?**
 - le correspondant doit avoir une certaine connaissance de la loi informatique et libertés et de l'informatique (mais pas de profil déterminé a priori)
 - ses qualifications doivent être précisées à la CNIL

LE CORRESPONDANT « INFORMATIQUE ET LIBERTÉS »: COMMENT LE NOMMER ?

- la désignation du correspondant doit être notifiée à la CNIL (recommandé avec AR)
 - Formulaire et guide pratique téléchargeable sur www.cnil.fr
 - Elle prend effet un mois après la notification
- Elle doit être portée à la connaissance des instances représentatives du personnel (recommandé avec AR)
- 175 désignations à ce jour; 75 correspondants.
- Un service de la CNIL dédié aux correspondants (N.Metallinos, H.Gudin)

LES DISPOSITIFS BIOMÉTRIQUES

- Donnée à caractère personnel: toute information relative à une **personne physique** identifiée ou susceptible de l'être, directement ou indirectement par référence à un numéro d'identification (ex: n° de sécurité sociale) ou un ou plusieurs éléments qui lui sont propres: initiales du nom et du prénom, date de naissance + commune de résidence, **données biométriques**: empreintes digitales, contour de la main, iris, reconnaissance faciale, ADN...

DISPOSITIFS BIOMETRIQUES: UN RÉGIME D'AUTORISATION PRÉALABLE

- Les traitements comportant des données biométriques doivent être autorisés par la CNIL (art. 25); ex: contrôles d'accès à des locaux, cantines scolaires, à des systèmes informatiques d'entreprises, gestion informatisée des horaires...
- Sauf ceux mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes qui doivent être autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la CNIL (art 27) ex: visas biométriques, contrôles d'accès à des locaux de ministères, préfectures...

LES DISPOSITIFS BIOMÉTRIQUES: LES 3 CRITÈRES D'APPRÉCIATION DE LA CNIL

- **1. Le type de biométrie : « à trace » ou « sans trace »**
 - la CNIL autorise les biométries « sans trace », (ex: contour de la main) car sans risque d'utilisation à l'insu des personnes (ex: contrôles d'accès à des locaux professionnels, à des cantines scolaires, dans un hôpital, au musée du Louvre, pour la gestion des horaires...)
 - Mais elle estime que les biométries « à trace » (ex: empreintes digitales, reconnaissance faciale, ADN...) présentent des risques car susceptibles d'être utilisées à l'insu des personnes, à d'autres fins.
 - Cf jugement du TGI de Paris du 19 avril 2005 ce Effia services et syndicat sud rail c.Société Effia services

LES DISPOSITIFS BIOMÉTRIQUES: LES 3 CRITÈRES D'APPRÉCIATION DE LA CNIL

- **2. Le mode de stockage de la donnée biométrique « à trace »: fichier ou support personnel**
 - le stockage dans un fichier de données biométriques telles que les empreintes digitales n'est admis **que pour des impératifs forts de sécurité et d'ordre public** (ex: zones sécurisées de la Banque de France, aéroport de Roissy, visas biométriques...)
 - La CNIL refuse le recours à des fichiers d'empreintes pour l'accès à des cantines scolaires, à un roller park, pour des systèmes de gestion des horaires dans un hôpital, une mairie...
 - Elle autorise les dispositifs de contrôle d'accès reposant sur un stockage des empreintes dans des cartes individuelles si des objectifs de sécurité le justifient (ex: locaux sécurisés de la poste, accès à des systèmes informatiques, accès par internet à des services financiers...)

LES DISPOSITIFS BIOMÉTRIQUES: LES 3 CRITÈRES D'APPRÉCIATION DE LA CNIL

- **3. Le consentement des personnes au stockage de leurs empreintes sur une carte**
 - Ex pour un programme de fidélisation des voyageurs
 - Mais comment s'assurer que ce consentement sera réellement libre et éclairé?

VIDÉOSURVEILLANCE: RAPPEL DU CHAMP DE COMPÉTENCE DE LA CNIL

- Sont soumis à la loi informatique et libertés;
 - Dans les lieux publics ou ouverts au public les enregistrements visuels de vidéosurveillance qui sont « utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques (art 10 I de la loi du 21 janvier 1995 modifiée).
 - Dans les lieux privés, les systèmes qui procèdent à la captation d'images au moyen d'un procédé numérique et à l'enregistrement de celles-ci sur un support numérisé ou encore les systèmes qui permettent l'alimentation de fichiers.

VIDÉOSURVEILLANCE: LES PROCÉDURES DE FORMALITÉS AUPRÈS DE LA CNIL

- L'application du régime de la déclaration normale;
- Mais une procédure d'autorisation en cas de système de vidéosurveillance couplé avec un dispositif de reconnaissance faciale (biométrie)

VIDÉOSURVEILLANCE: LES PRINCIPES À RESPECTER

- Le nécessaire respect du principe de proportionnalité: privilégier les objectifs de sécurité; pas de mise sous surveillance spécifique et permanente d'un employé ou d'un groupe d'employés;
- L'obligation d'information: pas de surveillance à l'insu des personnes; l'art 228-1 du code pénal prévoit une peine d'un an d'emprisonnement et de 45 000 euros d'amende le fait de porter volontairement atteinte à l'intimité de la vie privée d'autrui « en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé ».
- L'obligation de confidentialité: seuls les personnes dûment habilitées peuvent visionner les images; nécessité d'une durée de conservation limitée des images (ex: un mois).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

- 8 RUE VIVIENNE
CS 30223
75083 PARIS CEDEX 02
- TEL 01 53 73 22 22
- www.cnil.fr
- **Newsletter : infocnil**