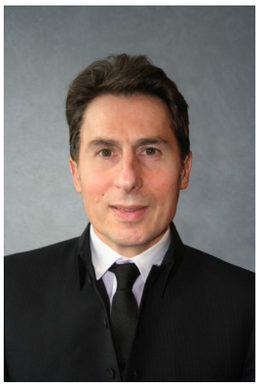
Maître Bensoussan répond à vos questions



Le 22 avril dernier, la formation contentieuse de la CNIL a ordonné l'interruption en urgence d'un dispositif de vidéo surveillance mis en œuvre par une société de transport routier. A la suite d'une plainte d'un salarié, la CNIL avait réalisé un contrôle et avait constaté que le dispositif plaçait le personnel sous surveillance constante générale et permanente...

La nouvelle organisation légale qui ressortira de la Loppsi 2 distingue la vidéosurveillance en deux catégories autonomes : la vidéosurveillance sur la voie publique dénommée vidéo protection et la vidéosurveillance dans le secteur privé. C'est dans ce second cadre que se situe la compétence de la CNIL. En effet, les systèmes de vidéosurveillance étant en général numériques, ils constituent un traitement automatisé de données et nécessitent donc toujours une déclaration préalable.

Dans l'affaire jugée par la Cnil, il apparaît que cette société avait mis en place un tel dispositif sans respecter l'ensemble des mesures imposées par la loi informatique et libertés à savoir, la déclaration à la CNIL, l'information des salariés, la consultation des représentants du personnel, le respect du droit d'accès aux enregistrements et la limitation de la durée de conservation à un mois sauf cas particulier. Dans ce cadre précis, la vidéosurveillance était de nature professionnelle : deux caméras filmaient en permanence le bureau d'exploitation comprenant les postes de travail des salariés et deux caméras avaient été installées sur le parking. Or, les constats effectués par la CNIL ont montré que la vidéosurveillance permanente du bureau d'exploitation était disproportionnée par rapport à l'objectif de sécurité. En effet, la vidéosurveillance doit avoir pour seule finalité, la lutte contre l'insécurité et non le contrôle d'activité des salariés. Compte tenu de cette situation, la CNIL a ordonné pour la première fois, l'interruption d'urgence du traitement de vidéosurveillance des salariés. Cette interdiction est fixée à 3 mois en l'application de l'article 45 de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La CNIL multiplie les contrôles pour garantir les droits des salariés. Ceci signifie t-il une augmentation des abus ?

Il n'y a pas plus d'abus mais souvent une incompréhension de la part des employeurs, du régime juridique applicable. Aujourd'hui, il est évident que la réforme de la vidéosurveillance n'entre pas dans les possibilités juridiques de l'employeur puisqu'il y a un risque de violation de la vie privée des salariés et qu'en France la réglementation est très protectrice. La vidéosurveillance doit être limitée à une zone particulière et doit avoir pour unique finalité la lutte contre l'insécurité. Elle n'a en aucun cas pour objet de faire du suivi d'activité des salariés. Si objectivement de plus en plus d'affaires apparaissent en milieu professionnel, cela provient du nombre de plus en plus important de caméras de vidéosurveillance installées au mépris de la réglementation ou en tout état de cause, de manière inappropriée (principe de proportionnalité et de pertinence).

Le 21 mai dernier, le Premier ministre a rappelé que le Gouvernement avait la ferme intention de généraliser les caméras embarquées à bord des véhicules de police, "parce qu'elles permettent de sécuriser les interventions des policiers par le suivi précis des opérations et le cas échéant, l'envoi rapide de renfort sur place ». Quelle législation en vigueur ?

La possibilité de doter des services de police et de gendarmerie d'un système d'enregistrement des opérations effectuées vise à prévenir toute contestation sur les modalités d'intervention des forces de l'ordre. En effet, aujourd'hui, avec les portables, toute personne a la possibilité de se transformer en cameraman d'exception. De ce fait, il est apparu nécessaire que le public présent auprès des victimes puisse présenter les images mais aussi et surtout les policiers ou gendarmes dans le cadre de leur intervention. On voit bien que la vidéo-enregistrement, comme la vidéosurveillance, présente deux phases : une phase de liberté et une phase de risque.

A cette fin, Michèle Alliot-Marie dans le projet de Loppsi 2 déposé en mai 2009, de même que François Fillon dans son discours du 21 mai 2010 sur le bilan de la politique du Gouvernement pour la sécurité, ont souhaité étendre l'expérimentation de vidéo embarquée dans les véhicules légers, engagée en 2006 dans la police nationale pour filmer les interventions dans les zones sensibles. Malheureusement, il semble que la commission des lois du Sénat qui a examiné, le 2 juin 2010, le rapport de Jean-Patrick Courtois et établi son texte sur le projet de Loppsi 2 n'a pas concrétisé de mesures en ce sens. C'était pourtant une bonne occasion de mener la réflexion demandée par la Cnil en avril 2008, sur l'enregistrement des paroles et des sons par les systèmes de vidéosurveillance embarquée. Dans une note adressée à Michèle Alliot-Marie, la Cnil constatant l'augmentation des demandes d'installation de systèmes de vidéosurveillance comportant la possibilité de procéder à l'enregistrement, outre des images, des paroles et des sons a demandé qu'une réflexion soit rapidement menée car les textes actuels d'application de la loi Pasqua et en particulier l'arrêté fixant des normes techniques, ne comportent aucune précision sur ce point.

Les expérimentations de vidéosurveillance "embarquées"

Loi n° 2006-64 du 23-01-2006, art. 8 et l'arrêté du 02-03-2007

Note annexe de la Cnil sur les exemples concrets de difficultés en matière de vidéosurveillance :

http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-Notevideosurveillance-ANNEXE.pdf

Certaines collectivités disposent d'un poste de contrôle central provisoire dépourvu de contrôle d'accès, dans l'attente d'un CSU… Ceci est-il légal ?

Le contrôle d'accès est un impératif, sauf dérogation particulière accordée par le Préfet, mais pour l'instant je n'en vois pas la justification. Le dossier de demande d'autorisation de mise en place d'un dispositif de vidéosurveillance prévoit expressément l'obligation de décrire les mesures prises pour contrôler l'accès au poste central (code d'accès, porte blindée, badge d'accès, accès contrôlé). En dehors de cette hypothèse de dérogation, on peut imaginer un dossier mal rempli ou un manque de vigilance…

Les députés ont adopté l'article 2 du projet de loi Loppsi qui vise l'usurpation d'identité sur Internet…

L'article 2 crée l'incrimination d'utilisation frauduleuse de données à caractère personnel de tiers sur un réseau de télécommunication.

Il existe déjà une loi d'usurpation à l'identité (voir encadré). Celle-ci a pour objet de reconnaitre la responsabilité pénale de la personne qui a usurpé un nom. Ces articles peuvent être utilisables dans le cadre juridique mais ce n'est pas forcément un cas d'application très simple. Dans le cadre du projet de Loppsi 2, toute usurpation d'identité à la personne « ou de toute autre donnée personnelle en vue de troubler sa tranquillité ou de porter atteinte à son honneur ou à sa considération » par le biais de communications électroniques notamment, a pour conséquence un risque de condamnation pénale, soit un an d'emprisonnement et de 15 000 € d'amende.

Ce texte s'oriente vers le respect de l'identité privée dans un cadre très général, aussi bien dans le monde réel que dans celui des octets.

La législation actuelle limite le délit d'usurpation d'identité au fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales (fraude informatique, escroquerie, abus de confiance, atteinte aux intérêt de l'Etat, etc.) notamment les articles 313-1, 314-1, 434-23 du Code pénal.