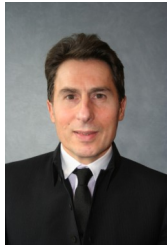


DROITS ET DEVOIRS...

Maître Bensoussan répond à vos questions



Les Webcams se déploient de façon considérable ces dernières années, notamment dans un but de promotion touristique, avec des résolutions de plus en plus proches de celles des caméras de vidéo protection. Cependant, il semblerait qu'il n'existe aucune juridiction à ce sujet...

La loi ne se prononce pas sur la technologie utilisée. Elle définit seulement les principales modalités de fonctionnement des systèmes et fixe des spécifications techniques. Cette absence de détermination des caractéristiques des dispositifs de vidéo protection a permis d'accompagner le développement des nouvelles technologies et d'appliquer la réglementation à des cas auxquels le législateur ne pouvait penser en 1995.

Concernant les webcams, la notice d'information relative au formulaire CERFA de demande d'autorisation distingue deux situations. Tout d'abord les systèmes de vidéo protection numériques dont les images sont transmises par internet et consultées, à distance, par les personnes responsables du système entrent dans le champ de la loi du 21 janvier 1995 ; le procédé numérique doit donc respecter des garanties imposées par la loi. Par contre, la diffusion sur internet d'images issues de webcams ne constitue pas un dispositif de vidéo protection dans la mesure où il n'y a pas « visionnage » des images sur un écran appartenant au propriétaire de la webcam mais une transmission directe sur internet. Ainsi, si la webcam est simplement un objet touristique avec transmission directe sur internet sans enregistrement et sans compression d'images, ce système ne relève pas de la vidéo surveillance, à condition que la webcam soit suffisamment loin des personnes de façon à ce qu'il n'y ait pas d'identification.

A contrario, lorsque les webcams sont orientées vers la voie publique, visionnent des personnes qu'on peut reconnaître, elles sont alors considérées comme illégales, constituant une violation de la vie privée (Art. 226-1 du code pénal).

Précisons que le piratage d'une webcam, processus simple et peu coûteux, est une atteinte à la vie privée passible d'un an d'emprisonnement et de 45 000 euros d'amende. Sont punies des mêmes peines, la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle, de dispositifs conçus pour la détection à distance des conversations, et permettant de réaliser l'infraction d'atteinte à la vie privée.

Enfin, même si cela ne relève pas de la vidéosurveillance, il est certain que la multiplication des caméras au domicile des particuliers modifie la frontière entre vie privée et vie publique...

De plus en plus de systèmes de vidéo protection sont équipés d'un microphone permettant, s'il est activé, d'enregistrer l'ambiance sonore du lieu à quelques dizaines de mètres à la ronde...

L'association du son et de l'image n'est pas prévue par la loi du 21 janvier 1995. L'arrêté du 26 septembre 2006 fixant des normes techniques minimales pour les systèmes de vidéosurveillance ne comporte aucune précision sur ce point. Et le projet de Loppsi 2 ne l'envisage pas davantage. Néanmoins, ce dernier vise à accroître la modernisation des forces de l'ordre « en intégrant pleinement les progrès technologiques ». Parmi les équipements qui seront développés pour faire face aux nouvelles menaces, figurent notamment : les générateurs de sons et les Taser équipés de caméras et de micros.

Si la captation sonore n'enregistre que des sons ambiants, comme la tempête, les bris de glace... c'est-à-dire tout ce qui est 'sonographique', on reste dans le domaine libre et ceci ne pose pas de problème. Par contre, on ne peut pas surprendre et enregistrer des conversations car ce serait une violation de la vie privée.

Rappelons que la sonorisation des lieux privés, est soumise à une déclaration CNIL ainsi qu'à une information des personnes concernées, la finalité étant la sécurité, la légitimité étant la lutte contre la fraude et la proportionnalité, le fait que les personnes puissent parler doucement.

Par ailleurs, l'enregistrement peut se faire uniquement en cas de mise en danger et de manière ponctuelle, c'est-à-dire jamais 24h/24. Enfin, le couplage de la vidéo avec différentes technologies (détecteurs de mouvement ou thermiques, sonorisation, technologie IP) apporte de nouvelles possibilités et des études sont en cours en ce qui concerne la fiabilité des systèmes de vidéosurveillance « intelligents ».

Le projet de loi Loppsi 2, s'il passe en l'état, va autoriser la surveillance d'ordinateurs privés à distance, sous le contrôle du juge d'instruction. Ainsi, l'article 23 permet de "mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères"...

Sur le plan technique, l'article 23 paraît s'inscrire dans une logique de lutte contre la fraude. Aujourd'hui, la surveillance est un principe qui n'est pas discuté lorsqu'il existe des faits concordants supposant une infraction. Le fait que la surveillance soit produite par des moyens informatiques, sans consentement des intéressés, sur des systèmes qui existent, sous réserve du contrôle du juge des libertés, me paraît s'inscrire dans l'utilisation normale des moyens qui aujourd'hui sont permis pour réaliser des enquêtes. Quelque part ici, nous ne sommes pas dans la notion d'espionnage mais dans la notion d'enquête et d'utilisation de l'ordinateur. Car il faut bien faire la distinction entre une enquête, qui suppose l'existence de présomptions de réalisations ou de pré réalisations internes d'une fraude ; et l'espionnage qui, en l'état actuel, est interdit, sauf infraction grave comme la lutte contre le terrorisme ou lorsque les impératifs de sécurité nationale sont en jeu. Ce qui est admis dans le cadre d'une enquête n'est pas tolérable à des fins privées ou des fins professionnelles. Car, il y a alors une véritable atteinte aux libertés individuelles, quand on peut piéger les personnes sans leur accord, sans autorisation contrôlée par le juge au titre de la protection.

La captation ne serait donc possible que dans le cadre d'une information judiciaire. Il serait ainsi impossible d'y recourir, sous peine de nullité de la procédure, selon la jurisprudence de la cour de cassation, dans le cadre d'une enquête (Cass. crim. 21/03/2007). Aujourd'hui, telle qu'elle est a priori envisagée, elle ne pourrait porter que sur un crime ou un délit relevant de la criminalité organisée entrant dans le champ de l'article 706-73 du code de procédure pénale.

Mais je pense que c'est une évolution naturelle et pas du tout une évolution liberticide de l'usage des nouvelles technologies, pour lesquels les principes essentiels sont toujours les mêmes et ne sont pas violés.

