Maître Bensoussan répond à vos questions

Un arrêté du 18 août 2011, publié au Journal officiel du 3 septembre, rend officiellement les policiers municipaux destinataires des données du fichier des véhicules volés "dans le cadre de leurs attributions légales" et dans le strict cadre de leurs fonctions, dans l'objectif, notamment, de permettre d'assurer une meilleure coordination entre policiers municipaux et policiers et gendarmes. Est-ce une véritable avancée, sur le plan juridique?

Aujourd'hui, une police moderne est une police informatisée qui échange des informations. Les fichiers constituent ainsi un des éléments déterminants qui contribuent à la politique de prévention et de répression. Il existe, dans ce cadre, plus d'une trentaine de fichiers dits « de police », dont celui des voitures volées n'est qu'une des illustrations.
Les fichiers de police sont aujourd'hui un des éléments incontournables permettant d'organiser la sécurité. L'enjeu, pour une démocratie, réside dans le fait de trouver la limite entre protection de la vie privée et sécurité des citoyens. Or actuellement, nous pouvons considérer que le principe de légitimité est en passe de dominer le principe de proportionnalité. Et l'extension de ce fichier, aux policiers municipaux, n'est qu'une illustration de cette situation. Avec le développement de la délinquance urbaine et le transfert d'une partie des charges y afférentes vers les collectivités locales, les policiers municipaux prennent des fonctions de plus en plus substituables à celles des policiers ou des gendarmes. Sur le terrain, la police municipale est en contact direct avec les citoyens et aussi avec les vols de voitures. Ainsi, du contrôle des parcmètres à celui des voitures volées, un nouveau pas est franchi. La CNIL a été consultée sur l'ouverture du fichier aux policiers municipaux et sa délibération du 15 juillet 2010 s'inscrit dans la recherche d'un équilibre visant à assurer la sécurité, l'intégrité et la sécurité des données, en recommandant notamment le chiffrement des données. La restriction d'accès des policiers municipaux, dans le strict cadre de leurs fonctions et attributions légales, est également un des éléments de garantie. En tout état de cause, la vitesse de développement des fichiers est inversement proportionnelle au développement du cadre juridique de leur régulation.

La Circulaire du 4 août 2011 porte sur la présentation des dispositions de la loi n° 2011-267 du 14 mars 2011 (LOPPSI II), relatives à la criminalité organisée et autres contentieux spécialisés (BOMJL n° 2011 -08 du 31.08.2011 - CRIM-2011-22-G1). Quelles sont les avancées apportées par cette circulaire ?
En ce qui concerne les données informatiques, la circulaire précise la philosophie de l'approche qui consiste à disposer de mécanismes juridiques d'intervention pour la police, permettant la captation de bout en bout de l'échange de données informatisées. En effet, si elle avait été prévue, en ce qui concerne les interceptions des télécommunications (interceptions de sécurité et interceptions judiciaires), la question de la captation des données se posait en aval et en amont de l'interception, c'est-à-dire lorsque la donnée n'était pas encore transmise sur les réseaux ouverts au public. Il en était ainsi des informations sur les PC, les tablettes, les unités de sauvegarde externes (clés USB, CD Rom), les réseaux locaux. En aval de l'interception, au sens juridique du terme, et en amont de l'interception, le texte sur la captation des données informatiques organise une possibilité de surveillance, de bout en bout.
Très souvent, le segment peut faire l'objet d'une interception de télécommunication (déchiffrement pour des raisons de sécurité judiciaire), alors qu'en général, les données en amont ou en aval ne sont pas chiffrées. La circulaire pointe donc effectivement cette possibilité de captation des données informatiques en indiquant que : « l'avantage de ce procédé est notamment de permettre la prise de connaissance du contenu du texte avant qu'il ne soit crypté ».

Un collège, à Colmar (Haut-Rhin) a mis en place un dispositif biométrique dans le but de contrôler l'accès des élèves à la cantine scolaire. Ce système ne laissant pas de trace, il a donc été autorisé par la CNIL, rendant alors impossible la constitution de fichiers ou l'utilisation de données personnelles à des fins abusives. Ce procédé est-il amené à se développer ou n'est-ce encore le fait de quelques expérimentations….
La généralisation de la biométrie dans les restaurants scolaires s'impose comme une solution simple efficace et peu coûteuse et touche aujourd'hui tous les systèmes à contrôle d'accès.
Il existe trois catégories de biométrie : la biométrie de sécurité, celle de confort et celle de confiance. Les dispositifs de biométrie apportant la sécurité sont réservés aux contrôles d'accès de lieux présentant des risques majeurs de sécurité, tels que les aéroports.
Les dispositifs de biométrie apportant le confort ne sont pas autorisés, dans la mesure où l'utilisation du corps humain comme moyen pratique de contrôle d'accès est considérée comme disproportionnée par rapport aux enjeux et n'est donc pas légitime. Par contre, les dispositifs de biométrie destinés à apporter la confiance sont dans une situation intermédiaire, à savoir qu'ils sont autorisés dès lors que les techniques utilisées ne présentent pas de risques d'usurpation d'identité. Tel est le cas de la biométrie par reconnaissance du contour de la main, autorisée depuis 2006 dans les établissements scolaires, car elle repose sur une biométrie dite « sans trace ». Un tel dispositif de biométrie est difficilement « détournable ». Pour qu'elle reste une biométrie acceptable, elle doit également être utilisée en tant qu'élément unique, c'est-à-dire sans utilisation de biométrie multimodale (combinaison des deux biométries, par exemple, reconnaissance combinée de l'empreinte digitale et du réseau veineux des doigts de la main). A partir de là, il est possible d'admettre, entre la biométrie dite « de sécurité » et celle dite « de confort », une 3e zone où l'on cherche à la fois de la confiance et de la sécurité.
La CNIL a refusé d'autoriser dans les écoles, au titre de la biométrie de confiance, l'utilisation de l'empreinte digitale car cette dernière peut être reproduite à l'insu de la personne concernée, puisqu'elle laisse des traces sur tous les supports qu'elle touche. A contrario, pour la biométrie de sécurité, la CNIL distingue les dispositifs en fonction du mode de stockage des empreintes digitales (avec ou sans maîtrise de la donnée par son détenteur).

Le site Copwatch (https://copwatchnord-idf.org/), site ayant pour objectif de surveiller la vie tant publique que privée des policiers et gendarmes, a créé une véritable polémique, ces dernières semaines, à tel moins que le ministère de l'Intérieur a déposé un référé visant à obtenir le blocage de ce site internet Copwatch, référé examiné le 12 octobre prochain. Que pensez-vous de ces nouvelles formes d'intrusion dans la vie des citoyens et d'étalage de faits ?
Le site Copwatch est une illustration de la banalisation des moyens d'enregistrement occultes dont plusieurs affaires célèbres ont montré les dérives (la fédération française de football, l'affaire Bettencourt, etc.). Cependant, à la facilité technique s'oppose une régulation juridique complexe.
En matière civile, lorsque les moyens utilisés sont contraires à l'ordre public, les enregistrements illicites ne peuvent être utilisés en tant que preuve, alors qu'en matière pénale, ils ne sont pas, par principe, rejetés. Ainsi, dans un arrêt du 18 mai 2010, la chambre criminelle de la Cour de cassation a admis l'enregistrement vidéo, provenant d'une source anonyme, comme mode de preuve licite, pour condamner un prévenu pour violences aggravées et participation avec arme à un attroupement. Cette situation crée une rupture dans le traitement du contentieux et la jurisprudence divergente qui en découle. En conséquence, chacun d'entre nous doit être maintenant conscient qu'il est sous enregistrement potentiel.
Toutefois, on peut s'interroger sur le fait de savoir si nous ne sommes pas en présence d'une nouvelle forme de régulation ? En effet, dans le site dont il est fait état, leurs auteurs dénoncent des actes illicites. Il faut donc trouver un point d'équilibre entre les potentialités croissantes de la technologie, et la garantie de certains droits fondamentaux tels le droit à la vie privée et à la protection des policiers dans le cadre de leurs fonctions, mais également, la présomption d'innocence des personnes filmées et l'interdiction de commettre des actes illégaux. La possibilité de dénoncer des actes illégaux est tout aussi un élément de régulation des démocraties, en ayant en mémoire de ne pas sombrer dans la délation.
Néanmoins, cette situation me paraît très singulière et je vous propose, après avoir étudié la question de manière beaucoup plus approfondie, de revenir vers vous ultérieurement, car il est nécessaire de réfléchir à des nouvelles organisations juridiques qui tiennent compte de l'ensemble des droits qu'il convient de conjuguer aux temps présents et à égalité.

A l'heure où nous mettons sous presse, nous apprenons que le délibéré de l'affaire Copwatch sera rendu vendredi 14 octobre à 17 heures. Une analyse en sera faite dans notre prochaine chronique.

Sources

Arrêté du 18 août 2011 modifiant l'arrêté du 15 mai 1996
Délibération n° 2010-299 du 15-7-2010

Circulaires.gouv.fr
Textes.justice.fr

Délibération n° 2006-103 du 27-4-2006
Cass. crim, 18 mai 2010, pourvoi n°09-83.156