Quand la vidéosurveillance européenne contredit la vidéoprotection française

x	Quand la vidéosurveillance européenne contredit la vidéoprotection française
---	--

L'arrêt rendu ce matin par la Cour de Justice de l'Union européenne en matière de vidéosurveillance risque d'avoir de douloureux effets en France. Il remet en effet en cause les efforts du ministère de l'Intérieur pour se passer de la CNIL dans l'installation des caméras de « vidéoprotection. »

Les faits examinés par la CJUE visait le cas d'un Tchèque ayant installé une caméra de surveillance chez lui, mais dont le champ de vision débordait sur la voie publique. Les flux étaient stockés sur disque dur, chez lui. Par ce biais, ce particulier avait finalement permis à la police d'identifier une personne suspectée d'avoir caillassé les fenêtres de sa maison. Cependant, la CNIL locale lui a infligé une amende, faute pour ce particulier d'avoir zappé le consentement préalable des personnes filmées. On pourra revoir notre actualité sur les solutions proposées par la Cour, mais l'important n'est peut-être pas là car l'arrêt est supposé provoquer un vent de panique en France, au ministère de l'Intérieur. Explication.

Vidéosurveillance, donnée personnelle, traitement automatisé

La Cour a en effet posé qu'en principe la vidéosurveillance relevait du champ d'application de la directive de 1995 sur les données personnelles, du moins « dans la mesure où elle constitue un traitement automatisé ». Cette analyse fait suite à un développement très logique :

La donnée personnelle embrasse « toute information concernant une personne physique identifiée ou identifiable. »

Est réputée identifiable « une personne qui peut être identifiée, directement ou indirectement, notamment par référence [...] à un ou plusieurs éléments spécifiques, propres à son identité physique. »

Du coup, « l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel (...) dans la mesure où elle permet d'identifier la personne concernée ». En clair, une caméra de vidéoprotection capte donc des données à caractère personnelles quand les personnes filmées sont identifiées ou identifiables.

Mais y a-t-il pour autant traitement automatisé de ces données ? La directive de 95 définit ce traitement par « toute opération ou [tout] ensemble d'opérations [...] appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement [...] la conservation ». La CJUE considère donc qu'« une surveillance effectuée par un enregistrement vidéo des personnes (...) stocké dans un dispositif d'enregistrement continu, à savoir le disque dur, constitue (...) un traitement de données à caractère personnel automatisé. »

Fort de ces enseignements, auscultons le régime français.

Les contrariétés du régime français de la « vidéoprotection »

Une circulaire du 14 septembre 2011 décrit le cadre juridique applicable à l'installation de caméras de vidéoprotection, terme officiel pour repêcher de manière plus sympathique les outils de vidéosurveillance. Cette circulaire est importante puisqu'elle définit les (rares) cas où les autorités doivent effectuer une déclaration préalable auprès de la CNIL, et quand elles peuvent (très souvent) s'en passer.

Deux hypothèses sont envisagées par cette circulaire qui vient faciliter l'application du Code de la sécurité intérieure : des caméras installées sur la voie publique, des caméras installées sur des lieux non ouverts au public.

Les caméras installées sur la voie publique

Les caméras installées sur la voie publique (et dans des lieux ou établissements ouverts au public) nécessitent l'autorisation préalable du préfet après avis de la commission départementale de la vidéo protection. Donc sans passer par la CNIL.

Cependant, parfois, ce passage CNIL est nécessaire. Le ministère de l'Intérieur, épaulée par un avis du Conseil d'État (non public et concernant les caméras dans les prisons) l'estime inévitable seulement « si les traitements automatisés ou les fichiers dans lesquels les images sont utilisées sont organisés de manière à permettre, par eux-mêmes, l'identification des personnes physiques, du fait des fonctionnalités qu'ils comportent (reconnaissance faciale notamment). »

Décodons : en France, lorsque le flux permet l'identification via un système de reconnaissance faciale (ou de plaque d'immatriculation), il faut passer par la CNIL. L'Intérieur en déduit naturellement que « le seul fait que les images issues de la vidéoprotection puissent être rapprochées, de manière non automatisée, des données à caractère personnel contenues dans un fichier ou dans un traitement automatisé tiers (par exemple, la comparaison d'images enregistrées et de la photographie d'une personne figurant dans un fichier nominatif tiers) ne justifie pas que la CNIL soit saisie préalablement à l'installation du dispositif de vidéoprotection lui-même. »

On le voit, ce point est en exacte contradiction avec ce que vient de juger la CJUE : des personnes, une caméra, un flux, un stockage, nous voilà déjà plongé jusqu'au cou en Europe dans le règne du traitement automatisé de données personnelles. La France, pourtant un État membre, estime qu'il n'y a pas de traitement automatisé (donc pas de passage par la CNIL) faute de flux couplé à une reconnaissance faciale ou de plaque d'immatriculation. Un critère totalement surabondant !

Les caméras installées dans les lieux non ouverts au public

La circulaire précitée évoque aussi les caméras installées dans les lieux non ouverts au public (soit partout ailleurs que les voies publiques, la résidence privée ou la voiture). Ce régime n'est pas de la compétence de l'Intérieur, mais celui-ci donne malgré tout des pistes : il faut là encore l'avis de la CNIL « lorsque ces personnes sont identifiables ».

La Place Beauvau pose ici deux critères cumulatifs :

D'une part des images qui font l'objet d'un enregistrement et d'une conservation, et non d'un simple visionnage.

D'autre part, une identification possible parce que le lieu est fréquenté par des personnes « dont une partie significative est connue du responsable du système de vidéoprotection ou des personnes ayant vocation à visionner les images enregistrées. »

Cependant, ces deux critères ne se retrouvent pas dans les textes fondateurs :

Si la captation n'est pas un traitement selon l'Intérieur, la loi de 1978 tout comme la directive disposent que la collecte et la transmission le sont bien.

Le critère de la « connaissance » des personnes filmées par celui derrière la caméra est quelque peu restrictif : une reconnaissance indirecte est normalement suffisante, d'autant que même si personne ne peut identifier Mme Michu sur son écran de contrôle, elle aura son image et pourra le faire par la suite.

Enfin, le critère de la « partie significative » n'est pas intégré dans les textes socles.

Bref, l'arrêt rendu ce matin par la CJUE devrait naturellement amener la CNIL à se pencher plus en profondeur sur le régime français, et l'Intérieur à revoir le périmètre de ses yeux électroniques. D'autres actualités seront à suivre en fonction des retours obtenus auprès de ces deux acteurs.

Consultez l'arrêt de la Cour de Justice de l'Union Européenne de l'affaire C-212/13

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.nextinpact.com/news/91367-quand-videosurveillance-europeenne-contrarie-vidioprotection-francaise.htm#page/1>
par Marc Rees