Maître Bensoussan répond à vos questions

Suite aux émeutes qui se sont déroulées, cet été, en Grande-Bretagne, la Métropolitain Police Service a diffusé des photos extraites des enregistrements Vidéo sur Internet, images correspondant aux personnes suspectées d'avoir commis des actes de vandalisme. Un appel a donc été lancé aux internautes. Juridiquement ce procédé est il légal? Ceci serait il également possible en France?

Votre question appelle trois niveaux de réponse. Tout d'abord, concernant l'utilisation des images de vidéoprotection, dans le cas des émeutes, la légitimité n'est pas discutable. Dans le cadre de cette utilisation, l'appel à témoins est une possibilité reconnue par la loi notamment lors d'enlèvements d'enfants : " Alerte Enlèvements ". Cependant, l'appel à témoignage vu sous l'angle de la "délation", pose la question de la délégation d'une fonction " régalienne " comme la surveillance générale de la voie publique qui doit être menée par les forces de l'ordre ([1]).

Enfin, le troisième élément de réponse à prendre en compte est celui relatif à l'atteinte à la vie privée en permettant à chaque citoyen de devenir un identificateur, voire un surveillant, à travers les images émanant des vidéos. Dans une démocratie, l'appel à la population pour aider la police doit avoir ses limites. Pour la paix sociale, il y a nécessairement une frontière à ne pas dépasser, même pour des besoins de sécurité. Aussi, je pense que l'utilisation des photos, avec appel à témoins en général, doit rester exceptionnelle, au regard d'événements exceptionnels.

Aujourd'hui, ce procédé est encadré par la loi sur la vidéoprotection qui limite le délai de conservation des enregistrements à un mois. En limitant les délais de conservation, on limite ainsi la généralisation de l'appel à témoins. Par conséquent, si l'événement n'est pas suffisamment prégnant pour apparaître dans ce délai, on préfère alors perdre des éléments probants concernant cet événement, plutôt que de garder les enregistrements : un équilibre a donc été trouvé. Et il est nécessaire que cet équilibre soit maintenu, à tous les niveaux, y compris en matière de reconnaissance faciale. Si la même situation s'était produite en France, on aurait également pu procéder à un appel à témoins. La Commission Nationale Informatique et des Libertés (CNIL) offre, me semble t-il, ce point d'équilibre qui existe déjà en matière de vidéosurveillance, à savoir le délai de conservation des images.

Si, à l'avenir, nous étions amenés à multiplier les appels à témoins, ne risquons-nous pas d'être confrontés au risque d'identifier des personnes susceptibles d'être suspectes alors qu'elles ne le sont pas dans la réalité ?

C'est un problème de compromis et d'équilibre à trouver. Ce qui doit nous guider, me semble t-il, c'est le caractère exceptionnel de l'événement et la dangerosité des faits. Mon propos s'appuie sur le principe de proportionnalité, pour lequel vous avez deux illustrations explicites à travers la limitation de conservation de certaines données : un délai d'un mois pour la vidéosurveillance et un délai d'un an pour les données de connexion. Vous remarquerez que ces deux délais ne sont pas alignés, car on a considéré, au titre de la proportionnalité, que le fait de regarder tous les visages dans la rue pouvait porter atteinte à la vie privée de façon plus importante que de tracer les données de connexion qui sont moins apparentes. Quoi qu'il en soit, appeler à témoignage sur reconnaissance faciale doit rester exceptionnel.

Et si une personne découvre sa photo sur Internet alors qu'elle n'a pas participé aux émeutes ?

Cette personne a, au minimum, trois moyens de recours : le 1er étant de demander immédiatement le retrait de cette information au titre de la loi pour la confiance dans l'économie numérique (responsabilité éditoriale des hébergeurs). La 2e possibilité est de saisir les tribunaux pour atteinte à la vie privée et droit à l'image (art. 9 du Code civil). Le 3e recours est celui lié au droit d'accès et de suppression, instauré par la loi informatique et libertés (art. 39 et 40 de la loi du 6 janvier 1978 modifiée en août 2004) . Elle dispose donc, au minimum, de trois recours extrêmement efficaces et rapides.

S'agissant de l'atteinte à la vie privée, il convient de remarquer que l'on se trouve face à la question de la responsabilité, lors de prises de photos dans la rue. Une personne marchant dans une rue est en déplacement privé, dans une zone publique. Aussi, le fait qu'elle soit " photographiable " ou que l'événement soit regardable, car s'affichant à l'extérieur, ne rend pas pour autant les informations " publiques ".

C'est uniquement parce que l'émeute est une manifestation publique, qu'on peut la prendre en photo. En dehors de ce contexte, la vidéosurveillance n'a pas le même régime juridique bien que ce soit la même technologie.

Le Ministère de l'Intérieur travaille à l'élaboration d'un fichier de reconnaissance faciale pour identifier les suspects, grâce à l'utilisation des images vidéo. La Cnil a été saisie. D'après vous, quelles seront ses conclusions ?

Une expérimentation est en cours ([2]) en ce qui concerne le traitement de données à caractère personnel ayant pour objet la reconnaissance faciale en temps réel de personnes en environnement non contraint.

Cette expérimentation, réalisée sous la maîtrise du ministère de l'Intérieur et du cabinet du préfet de police de Paris, consiste autoriser la reconnaissance faciale, sur des images provenant de vidéosurveillance, dans le cadre d'une prise de vue dans des espaces non contraints -(à savoir, sans passage par des portiques) le plus souvent dans des stades sportifs. Sans préjuger de la décision de la Cnil, lorsque cette expérimentation, limitée à 36 mois, aura fait ses preuves, il est fortement probable qu'elle devienne définitive. Pour moi, c'est irréversible car la reconnaissance faciale, sous réserve du respect du principe de proportionnalité, a une finalité de sécurité tout à fait légitime.

Certains critiquent cette technologie, les résultats n'étant pas toujours fiables…

Ce type d'argumentaire n'a pas beaucoup de sens, car il se situe dans le cas d'une preuve unique. Or, on ne peut avoir de preuve unique en matière d'identification judiciaire. Il ne peut s'agir que d'une preuve de type " probabiliste ". A titre d'exemple, prenons trois niveaux de réflexion probatoire : en France, la loi exige qu'une empreinte ait une concordance d'au moins 15 minuties ([3]) pour être considérée comme preuve judiciaire. Actuellement, on identifie des personnes par empreinte digitale à 10^{-4} près ; une peine de prison peut être prononcée à partir notamment d'une empreinte génétique qui est différentiante à 10^{-9} près. Avec les outils de cryptographie permettant d'assurer les fonctions d'authentification, de non-répudiation et d'intégrité, on est sûr de l'identification des parties à 10^{-11} près.

La reconnaissance faciale offre un taux de probabilité qui reste raisonnable. Il est certain que nous sommes toujours confrontés à un problème entre le " faux vrai " et le " vrai-faux ". Mais, il faut prendre en compte le fait que nous ne sommes jamais confrontés à des preuves uniques, ces preuves étant toujours situées dans un contexte. La preuve, en matière pénale, est dominée par plusieurs principes fondamentaux et notamment, l'intime conviction du juge tempérée par celui de la présomption d'innocence. Un minimum de charges susceptibles de fonder l'intime conviction du juge doivent être réunies. Il ne saurait y avoir de condamnation brutale sur une probabilité.

[1] Lors du contrôle de légalité de la LOPPSI 2 cette question avait été soulevée par le Conseil Constitutionnel pour censurer les dispositions qui permettaient le visionnage des images par des agents d'opérateurs privés, Décision 2011-625 DC du 10 mars 2011 :
http://www.alain-bensoussan.com/wp-content/uploads/21863652.pdf

[2] Délibération n° 2010-097 du 8 avril 2010 :
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000022205713&fastReqId=1885294986&fastPos=4

[3] Les minuties sont des marques cutanées particulières formant des figures comme des lacs, des fins de traits, des bifurcations dans les crêtes ou encore des crochets. Source : INPS (Institut national de police scientifique) :
http://tpe-inps.e-monsite.com/rubrique,3-empreintes-digitales,267499.html