

## **Vidéo-surveillance, vidéo-protection et biométrie : Comment équilibrer droit à la vie privée et droit à la sécurité ?**

Charly LACOUR, Doctorant contractuel en Droit

**Université de La Rochelle**

Le 19 septembre 2018, la Commission Nationale Informatique et Libertés (Cnil), publiait un communiqué<sup>1</sup> appelant le Législateur à se saisir des questions posées par les nouveaux outils utilisés dans le cadre de la prévention des troubles à l'ordre public. Étaient notamment visés les dispositifs de vidéo surveillance couplés à l'usage du big data et de données biométriques.

Lorsque de tels dispositifs sont utilisés par des personnes morales de droit privé, le RGPD trouve à s'appliquer. Ainsi, les données recueillies et utilisées à des fins de reconnaissance faciale sont considérées comme des données biométriques au sens de l'article 4-14 dudit règlement : « données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ». Que le dispositif soit utilisé comme moyen d'identification ou d'authentification, par une société pour contrôler l'accès à ses locaux ou par une personne physique pour déverrouiller son smartphone, cette dernière doit pouvoir conserver un contrôle sur son « gabarit » (jeu de données la concernant), et dans le cas de technologies grand public, pouvoir utiliser son terminal sans recourir obligatoirement à une authentification par biométrie. Dans les différents cas de figure, et en l'attente des référentiels RGPD, la Cnil permet aux responsables de traitement de se référer à ses anciennes « autorisations uniques » ( par exemple : Autorisation unique AU-053 : Biométrie : Contrôle d'accès sur les lieux de travail, avec conservation des gabarits biométrique en base<sup>2</sup>).

La question devient beaucoup plus complexe lorsque ces outils basés sur la biométrie ou des données sensibles en général sont utilisés à des fins de prévention des troubles à l'ordre public. Le programme Reporty, expérimenté par la ville de Nice, va tester un système de reconnaissance faciale auprès de 1 000 volontaires. « Six caméras seront implantées dans un corridor d'accès au carnaval organisé entre le 16 février et le 2 mars. Elles scruteront les visages pour tenter de détecter, trois jours durant, une correspondance entre

1 « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », 19/09/ 2018, [cnil.fr](http://cnil.fr)

2 <https://www.cnil.fr/fr/declaration/au-053-biometrie-controle-dacces-sur-les-lieux-de-travail-avec-conservation-des-gabarits>

les vidéos et des photos fournies préalablement par ces cobayes »<sup>3</sup>.

Dans ce contexte, ce n'est plus le RGPD qui va trouver à s'appliquer, mais la directive n° 2016/680 du 27 avril 2016, dite directive « Police-Justice », transposée par la loi n° 2018-493 du 20 juin 2018, venue modifier la loi Informatique et Libertés. La directive, en son article 10, vient autoriser l'usage de ces dispositifs de surveillance « uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée (...). De tels dispositifs ont d'ores et déjà été autorisés en France, « au coup par coup »<sup>4</sup>, mais concernent essentiellement les caméras piéton ou la captation d'images fixes sans forcément avoir recours à la reconnaissance faciale, comme cela est expérimenté à plus grande échelle en Chine, notamment<sup>5</sup>.

Dans son communiqué du 19 septembre 2018, « la CNIL appelle d'urgence à un débat démocratique sur cette problématique, et à ce que le législateur puis le pouvoir réglementaire se saisissent de ces questions afin que soient définis les encadrements appropriés, en recherchant le juste équilibre entre les impératifs de sécurisation, notamment des espaces publics, et la préservation des droits et libertés de chacun »<sup>6</sup>.

Alors que le RGPD vient apporter bon nombre de réponses, tant techniques que juridiques dans la sphère privée, un tel débat, incluant pénalistes, juristes spécialisés et techniciens permettrait, dans la sphère publique, que « le droit ne court plus après la technologie »<sup>7</sup>.

3 « Reconnaissance faciale : la ville de Nice n'a pas reçu « d'autorisation » de la CNIL », Marc Rees, Next impact, 19/02/2019

4 « Reconnaissance faciale : « Le droit court un peu après la technologie » », Laurence Neuer, Le Point, 19/10/18, entretien avec Jean Lessi, secrétaire général de la Cnil

5 « En Chine, le grand bond en avant de la reconnaissance faciale », Elsa Trujillo, Le Figaro, 11/12/17

6 *Cf note 1*

7 Jean Lessi, « Reconnaissance faciale : « Le droit court un peu après la technologie » », Laurence Neuer, Le Point, 19/10/18, entretien avec Jean Lessi, secrétaire général de la Cnil