Police, caméras et algorithmes : Comment assurer le respect des droits fondamentaux dans le cadre de l'utilisation des outils de police « prédictive » ?

Laurène BAUDOUIN, Université de Lille, CERAPS-UMR CNRS 8026

- **Communauté d'appartenance**

Doctorante en droit public et spécialisée en droit du numérique, je contribue dans le cadre de différents projets à identifier et analyser les aspects juridiques impliqués. Les sujets traités incluent notamment la protection des données à caractère personnel, les algorithmes, la cybersécurité ou encore les drones.

- **Contribution à l'atelier**

À l'origine, le recours aux caméras filmant l'espace public constitue l'une des principales réponses apportées aux besoins exprimés par les forces de police et de gendarmerie en vue d'assurer le maintien de l'ordre public. L'introduction de caméras utilisées à des fins de surveillance doit son origine à la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité[1] (LOPS), première loi relative à la « vidéosurveillance » de la voie publique. Ces caméras occupent depuis lors une place prépondérante dans le cadre des activités des forces de l'ordre au motif qu'elles permettent d'assurer une meilleure sécurité des personnes et de leurs biens ainsi qu'à préserver les libertés de chacun. Leur régime juridique fut ensuite approfondi par la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure[2] (LOPPSI 2) introduisant le Code de la sécurité intérieure (CSI) et effectuant un changement sémantique du terme de « vidéosurveillance » à celui de « vidéoprotection ». Par ailleurs, cette nouvelle terminologie ne dissimule pas la volonté politique de présenter une image plus protectrice de ces outils plutôt que celle d'un État de surveillance.

Les importantes manifestations politiques qui ont eu lieu ces deux dernières années associées au climat national de lutte contre le terrorisme sévissant depuis 2015 ont favorisé l'engouement pour

[1] Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, JORF n° 0020 du 24 janvier 1995.

[2] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n°0062 du 15 mars 2011.

les technologies de surveillance et notamment le recours aux caméras. De fait, le nombre de caméras entrant dans le cadre de la vidéoprotection est en croissance constante et ne se limite plus aux seuls dispositifs fixes. Il en va ainsi des caméras individuelles (aussi désignées sous les termes de « body cam ») dont peuvent se doter les agents des forces de l'ordre lors de leurs interventions[3]. Enfin, les drones ont commencé à faire leur apparition offrant des opportunités considérables tant sur le plan opérationnel que concernant la collecte d'informations. Les systèmes de vidéoprotection sont une source intarissable de données principalement à caractère personnel, par conséquent, ils sont soumis à la loi Informatique et libertés du 6 janvier 1978[4] (LIL) et dans le cadre d'une utilisation à des fins de maintien de l'ordre public à la Directive européenne concernant le traitement des données à caractère personnel par les autorités compétentes dans le cadre pénal du 27 avril 2016[5] (aussi appelée Directive « Police-Justice »).

Pour autant, les systèmes de vidéoprotection ne se contentent plus seulement de collecter des données mais ne cessent d'évoluer. Ainsi, les algorithmes se sont progressivement invités au sein des outils de vidéoprotection. Une des premières facultés dont ont été dotées les caméras de surveillance fut notamment la très controversée reconnaissance faciale suscitant de nombreux débats et un rappel à l'ordre de la Commission nationale informatique et libertés (CNIL) invitant à des débats approfondis afin de répondre aux inquiétudes qu'elle suscite[6]. Parmi les préoccupations qu'elles engendrent se trouvent inévitablement le droit au respect de la vie privée, la liberté d'aller et venir mais aussi d'autres droits fondamentaux. Toutefois, les algorithmes ne se limitent pas à la reconnaissance faciale et se destinent progressivement à la détection d'individus et d'objets en mouvement allant jusqu'à l'étude du comportement humain. En ce sens, plus qu'à identifier une personne dans un premier temps, les autorités de maintien de l'ordre public cherchent désormais à anticiper les évènements. Certains auteurs parlent alors de police « prédictive ». Il convient, cependant, d'utiliser ces termes avec précaution tant la « prédiction » sous-entend une vision certaine du futur qui pourtant ne l'est pas. La police « prédictive » se fonde sur des algorithmes prédictifs dont l'objectif consiste à anticiper des événements en utilisant de manière plus efficace et en agrégeant des données historiques à de nouvelles informations[7]. Ces outils de police « prédictive » n'en sont encore qu'à leurs débuts mais devraient être en mesure de s'adapter très prochainement à tous types d'événements. Ces algorithmes visent à analyser une situation en cours

---

[3] Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, JORF n°0129 du 4 juin 2016.

[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 janvier 1978, modifiée par la loi du 20 juin 2018.

[5] Directive (UE) n°2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, J.O L 119, 4 mai 2016, pp. 89-131.

[6] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », 15 novembre 2019 [https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux].

[7] CASTETS-RENARD, Céline, « L'IA en pratique : la police prédictive aux États-Unis », *Dalloz IP/IT*, n°5, 15 mai 2019, p.314.

en s'appuyant sur un historique de données issues de son apprentissage et sur les données collectées en cours de mission. Les algorithmes peuvent alors être confrontés à plusieurs difficultés. En premier lieu, l'algorithme peut contenir des failles créant à terme un résultat erroné pouvant porter préjudice aux personnes concernées. Les exemples d'erreurs en matière de reconnaissance faciale ne manquent pas à ce sujet et démontrent une certaine précipitation dans l'échantillonnage proposé à l'algorithme lors des phases d'apprentissages. En deuxième lieu, les données collectées durant la mission peuvent être insuffisantes ou défectueuses. Enfin, les données issues des fichiers de police peuvent comporter des erreurs susceptibles d'entrainer de faux résultats de l'algorithme. L'analyse de données par ces algorithmes devront, à terme, mener à une analyse en temps réel du comportement qu'il s'agisse de détecter les mouvements de foule ou le comportement dit « anormal » d'un individu. Or, le manque de fiabilité dont ils font encore preuve laisse présager de potentielles atteintes aux libertés fondamentales et particulièrement la liberté individuelle.

Le 15 janvier 2020, une Proposition de loi constitutionnelle relative à la Charte de l'intelligence artificielle et des algorithmes[8] a été émise. Bien que démontrant une volonté de réguler l'utilisation des algorithmes, cette charte suffira-t-elle à répondre aux nombreuses interrogations que soulève l'introduction des algorithmes au sein des outils de vidéoprotection ? Il apparait donc nécessaire de remettre l'être humain au cœur de ces enjeux et de la chaine décisionnelle.

[8] Prop. de loi n° 2585 constitutionnelle relative à la Charte de l'intelligence artificielle et des algorithmes, enregistrée à la présidence de l'Assemblée nationale le 15 janv. 2020, présentée par P.-A. Raphan [http://www.assemblee-nationale.fr/dyn/15/textes/l15b2585_proposition-loi.pdf].