



Paris, le 10 mars 2022

Caméras “intelligentes” : N’ouvrons pas de nouvelle brèche dans notre État de droit

Contribution à la consultation publique de la Commission nationale de l’informatique et des libertés sur sa position relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics

Cette contribution repose notamment sur les travaux engagés par le think tank Renaissance Numérique sur l’utilisation des technologies numériques à des fins de sécurité¹. Bien que la Commission nationale de l’informatique et des libertés (CNIL) ne s’intéresse pas qu’à cette seule finalité dans sa position sur l’utilisation des caméras dites “intelligentes” ou “augmentées”, plusieurs enseignements peuvent être tirés de ces réflexions.

1. Le cadre existant offre déjà la possibilité à la CNIL de contrôler le déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics

Le cadre juridique qui entoure le déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics est particulièrement fourni : Règlement général sur la protection des données (RGPD), Directive Police-Justice, Loi Informatique et Libertés, Code de la sécurité intérieure (vidéoprotection), Convention européenne de sauvegarde des droits de l’homme et des libertés fondamentales, Charte des droits fondamentaux de l’Union européenne, Constitution, jurisprudence de la Cour de justice de l’Union européenne (CJUE), de la Cour européenne des droits de l’homme (CEDH) et du Conseil d’État, etc.

¹ “Technologies de sécurité : Sans un contrôle effectif, pas de confiance des citoyens”, Renaissance Numérique, juin 2021 : <https://www.renaissancenumerique.org/publications/technologies-de-securite-sans-un-controle-effectif-pas-de-confiance-des-citoyens> ; “Reconnaissance faciale : Porter les valeurs de l’Europe”, Renaissance Numérique, juin 2020 : <https://www.renaissancenumerique.org/publications/reconnaissance-faciale-porter-les-valeurs-de-l-europe>

Un cadre juridique très clair régit déjà les principes de finalité et de proportionnalité et s'applique au déploiement de ces technologies. Une mesure restreignant les droits et libertés respecte ce qu'on appelle le triple test, c'est-à-dire qu'elle doit être à la fois : appropriée, en ce qu'elle doit permettre de réaliser l'objectif légitime poursuivi ; nécessaire, c'est-à-dire qu'elle ne doit pas excéder ce qu'exige la réalisation de cet objectif ; et proportionnée, en ce qu'elle ne doit pas, par les charges qu'elle crée, être hors de proportion avec le résultat recherché.

La méthode d'application de ce principe permet d'évaluer la nécessité ou les apports mesurables (en qualité, en pertinence, en efficacité) des technologies utilisées au regard des objectifs visés, afin de garantir les libertés publiques en vérifiant que les finalités envisagées correspondent aux missions qui sont dévolues.

Ce cadre permet notamment à la Commission nationale de l'informatique et des libertés de contrôler ces déploiements en tenant compte de leur impact sur les droits et libertés fondamentales, la protection de la vie privée et la protection des données à caractère personnel pour lesquelles elle est compétente. **Encore faut-il penser l'articulation de ce cadre - par exemple entre le RGPD, la Directive Police-Justice et la réglementation entourant la vidéoprotection - et donner à la CNIL les moyens de ses missions de régulation.**

En l'état du droit français en vigueur, seule la décision d'installation de caméras filmant un espace ouvert au public, relève d'une compétence préfectorale héritée de la loi de 95-73. Cependant, la détermination du lieu et celle de la finalité d'installation d'une caméra ne sauraient à elles seules déterminer la proportionnalité de l'exploitation des images qui en seront issues.

La CNIL dispose depuis 1978 et aujourd'hui encore en application du RGPD - comme ses homologues européens - d'une pleine compétence sur la collecte et l'utilisation des signaux (images, sons, mouvements et formes) captés par ces caméras et résultant des technologies associées à celles-ci. Analyse automatisée de l'image, dispositifs de détection d'évènements ou de mouvements, de formes, de silhouettes, d'attitudes ou de visages, biométrie et reconnaissance faciale, la compétence et l'indépendance de la CNIL sur ces usages et ces technologies ne sauraient être remises en cause, dès lors que ces signaux donnent lieu ou sont issus d'un traitement de données à caractère personnel. Cette compétence de la CNIL précède même l'analyse du caractère anonyme ou non personnel d'une donnée, le RGPD et la loi 78-17 "Informatique & Libertés" lui conférant de manière exclusive en France le soin de déterminer si et quand une donnée n'a pas ou plus de caractère personnel, sous le contrôle ultime du Conseil d'Etat.

C'est donc le respect même du cadre applicable qui fait défaut en pratique et non le manque de cadre. La Commission nationale de l'informatique et des libertés doit être confortée dans sa mission, à la fois par des moyens adéquats et une légitimation de ses avis et démarches de contrôle. Ses capacités d'action demeurent encore trop limitées et surtout en décalage par rapport à la profondeur de son champ de contrôle. Réaliser des analyses d'impact portant sur des technologies complexes est une tâche chronophage qui requiert des ressources significatives, non seulement budgétaires, mais également (et de façon tout aussi importante) humaines (personnel hautement qualifié) et pluridisciplinaires (expertises juridiques, sectorielles et techniques).

La problématique ici relève donc plutôt du budget et des priorités politiques accordées à la préservation des droits et libertés dans notre société, que de la création d'une loi *ad hoc*

dédiée à des technologies spécifiques. Cette approche réduite à une catégorie de technologies dans un contexte particulier a depuis très longtemps systématiquement démontré son inefficacité et son impact négatif sur l'accompagnement de l'innovation, engendrant des incohérences et des compétitions réglementaires au détriment de la maturité et de la souplesse des approches holistiques.

Le risque d'une nouvelle loi serait d'ouvrir une nouvelle brèche dans le cadre protecteur de notre État de droit, à l'instar des récentes lois liées à la sécurité et au renseignement, à la santé connectée ou aux parcours éducatifs.

Un dernier exemple en date est la proposition de loi pour une sécurité globale préservant les libertés pour laquelle nombre d'acteurs, en dépit de son intitulé, ont soulevé les risques pour les libertés publiques. Dans sa décision du 20 mai 2021², le Conseil constitutionnel a invalidé plusieurs articles de la proposition de loi (7 articles sur 22), dont certains relatifs à l'emploi de technologies numériques par les forces de l'ordre. Le juge constitutionnel a relevé ainsi plusieurs atteintes à l'équilibre entre « *les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions et le droit au respect de la vie privée* ». Le fait qu'il se soit agi d'une proposition de loi et non d'un projet de loi n'a d'ailleurs rien d'anecdotique et a permis à l'exécutif et au législateur d'échapper à l'obligation de conduire une analyse d'impact.

Notons à ce titre qu'une éventuelle loi dédiée à ces caméras en raison de leur caractère "intelligent" ou "augmenté" ouvrirait un nouveau paradigme juridique : dès lors qu'on ne régulerait plus seulement la collecte d'images (principe actuel), mais également le fait de les interpréter ("*capacité de détection et d'analyse*"³). **On s'inscrirait clairement dans un texte de contournement des compétences de la CNIL établies depuis 1978**, non conforme à l'ensemble des traités internationaux conclus par la France depuis lors et confiant à une autorité indépendante à compétence générale, le soin de réguler les traitements de données personnelles.

Or, aucune interprétation d'une image, d'un son ou d'un mouvement, si innovante, automatisée et intelligente soit-elle, ne saurait passer l'examen de proportionnalité d'une technologie au seul motif de la finalité qu'elle sert. De surcroît, aucune loi, si forte soit-elle en termes de garanties et de restrictions, ne saurait renvoyer uniquement à un mécanisme contentieux - pour violation de la loi -, alors que l'examen souple et constructif de ses conditions d'application est une tâche durable que n'éteint pas un débat législatif ni un contentieux ponctuel. C'est par l'intervention d'un organe de régulation permanent - qui existe déjà, la CNIL -, disposant d'une expertise particulière et de moyens adéquats, que nos valeurs peuvent s'incarner dans des prises de décision contextuelles, adaptées et utiles.

Recourir à des lois spéciales ayant pour unique vocation de contourner la compétence de régulateurs en place, ne gagne ni du temps ni de l'efficacité à l'encadrement de l'innovation et des débats de société. S'en remettre aux conclusions d'un contentieux atypique pour défaire *a posteriori* des dispositifs qui n'avaient pas lieu d'être, sans sécréter de pistes de validité pour

² Conseil constitutionnel, Décision n° 2021-817 DC du 20 mai 2021 : <https://www.conseil-constitutionnel.fr/decision/2021/2021817DC.htm>

³ Extrait de la position de la CNIL.

l'avenir, n'est pas davantage utile, ni à la sécurité, ni à nos libertés. Il n'est pas sain ni efficace de remplacer la nécessaire recherche des équilibres sociétaux par une alternance destructrice entre des aventures législatives temporaires et des recours européens ou des questions prioritaires de constitutionnalité, qui font et défont, à quelques années d'intervalle, ce que nos sociétés démocratiques ont besoin de construire dans la durée, à savoir l'accompagnement de l'innovation et de l'efficacité publique dans le respect concret - factuel et vérifiable - de nos principes fondamentaux.

2. L'encadrement de ces technologies dépasse le seul cadre de la protection des données

S'il convient de noter que l'analyse de la conformité de ces technologies aboutira toujours à l'enjeu de la protection des données personnelles, l'utilisation des caméras dites "intelligentes" ou "augmentées" peut avoir un impact sur d'autres droits fondamentaux (liberté de réunion et d'association, liberté de circulation, non-discrimination, légalité des délits et des peines, égalité devant la loi, recevabilité des preuves, procès équitable, non-discrimination, etc.). Ce contrôle de la conformité doit donc passer par une analyse fine des risques associés à l'emploi de telle ou telle technologie dans un contexte spécifique, c'est-à-dire **la vérification opérationnelle que les droits et libertés fondamentales sont bien respectés** dans un contexte mouvant. À ce titre, le recours au triple test a toujours permis de faire une évaluation essentielle en termes de compatibilité des usages avec l'ensemble des droits et libertés fondamentales. Ainsi, d'autres autorités compétentes telles que le Défenseur des droits dans son domaine de compétence recourent à cet examen.

Cet enjeu méthodologique a fait ses preuves d'utilité et d'efficacité, car il permet de passer l'emploi de technologies au tamis du triple test, en élaborant des contextes et des "cas d'usage", dès la conception des technologies et avant leur mise en œuvre. Il s'agit donc d'aller plus loin qu'une régulation *ad hoc* qui risquerait de fragiliser notre cadre juridique, en appliquant en amont une logique de conformité ou de prohibition au regard des nos droits et libertés fondamentales (droits et libertés *by design*). **Il s'agit d'intégrer des critères d'analyse sur la base du triple test dans la standardisation⁴** en amont - une standardisation qui ne peut être construite qu'au niveau européen pour être pertinente -, et en aval, d'infléchir le cadre de la commande publique afin de préserver des avantages compétitifs illustrant nos valeurs, plutôt que de renoncer à celles-ci *ab initio*, sans permettre à une concurrence saine de s'établir. Concrètement, il s'agit d'octroyer des marchés publics aux seuls acteurs respectant les standards en question, pour toutes les caméras dites "intelligentes" ou "augmentées". S'agissant de technologies évolutives, leur conformité aux standards devra être par ailleurs régulièrement évaluée, ainsi que les standards

⁴ Renaissance Numérique a fait une proposition sur la standardisation dans son rapport relatif aux technologies de reconnaissance faciale. "Reconnaissance faciale : Porter les valeurs de l'Europe", Renaissance Numérique, juin 2020 : <https://www.renaissancenumerique.org/publications/reconnaissance-faciale-porter-les-valeurs-de-l-europe>

eux-mêmes. À ce titre, Renaissance Numérique dans son rapport dédié à la reconnaissance faciale a proposé un schéma de gouvernance qui peut être appliqué pour ces technologies⁵.

Réguler ce n'est pas interdire, contourner ou renoncer. C'est permettre, dans un cadre lisible et stable pour quiconque.

Rédaction

⁵ Voir à la page 91 du rapport. "Reconnaissance faciale : Porter les valeurs de l'Europe", Renaissance Numérique, juin 2020 : <https://www.renaissancenumerique.org/publications/reconnaissance-faciale-porter-les-valeurs-de-l-europe>