N° 472864
Commune de Beaucaire

10ème et 9ème chambres réunies

Séance du 5 avril 2024
Décision du 30 avril 2024

CONCLUSIONS

M. Laurent DOMINGO, Rapporteur public

La videoprotection (sur la voie publique ou les lieux ouverts au public) et la vidéosurveillance (lieux non ouverts au public), alors qu'elles sont largement répandues, génèrent cependant peu de contentieux devant vous[1]. Ce n'est toutefois pas parce qu'elles ne posent pas de difficultés de mise en œuvre, comme le montrent les décisions, de mise en demeure ou de sanctions, rendues en la matière par la CNIL[2], qui a d'ailleurs fait des caméras augmentées, c'est-à-dire des systèmes de captation d'images assortis de logiciels de traitements automatisés des images en vue de produire des informations, un axe prioritaire de son plan stratégique 2022-2024 et une thématique de ses contrôles de l'année 2023. Le recours de la commune de Beaucaire contre la mise en demeure que lui a adressé la présidente de la CNIL à propos notamment de son système de videoprotection équipé d'un dispositif de lecture automatisé des plaques d'immatriculation (LAPI) va vous donner l'occasion d'aborder certaines de ces difficultés.

A l'occasion d'un contrôle de l'ensemble de la politique de la commune en matière de données personnelles, engagé à la suite d'un signalement de la Chambre régionale des comptes, les services de la CNIL ont estimé que la commune ne respectait pas plusieurs de ses obligations résultant du RGPD[3] et de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment s'agissant de son système de videoprotection. A l'issue de ces opérations de contrôle, la présidente de la CNIL, sur le fondement de l'article 20 de la loi du 6 janvier 1978, a adressé à la commune, le 6 février 2023, une mise en demeure de se

[1] Pour un refus d'autorisation d'installer un système de videoprotection, v. par ex. 27 juin 2016, Commune de Gujan-Mestras, n°385091, p. 256 ; en QPC, v. 5 février 2024, Syndicat mixte ouvert Seine-Et-Yvelines Numérique, n°489300 ; pour une clôture de plainte par la CNIL, v. 27 mars 2023, D..., n° 467774, B ; pour une sanction prononcée par la CNIL, v. 30 janvier 2024, Société LHA Développement, n° 473254 ; pour la surveillance par drones, v. 22 décembre 2020, Association La Quadrature du Net, n°446155, T. p. 750

[2] v. Rapport de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, Sénat, n° 248, p. 40.

[3] Règlement n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

conformer à plusieurs obligations en matière de données personnelles. La commune de Beaucaire vous demande d'annuler cette mise en demeure.

I. Avant d'aborder les questions relatives à la videoprotection, nous traiterons des autres manquements au droit des données relevés dans la mise en demeure et contestés par la commune.

A. Plusieurs demandes de la commune peuvent s'écarter ensemble car elles appellent la même réponse négative.

En effet, la commune, en ce qui concerne le registre des activités de traitement, qu'elle n'avait pas élaboré, en méconnaissance de l'article 30 du RGPD, ou la définition des durées de conservation des données qu'elle traite, qu'elle n'avait pas définies en méconnaissance de l'article 5 du RGPD, ou encore la gestion sécurisée des mots de passe et la réalisation d'une analyse d'impact sur la protection des données traitées par le centre communal d'action sociale, demande l'abrogation de la mise en demeure au motif qu'elle s'y est conformé.

Mais il n'y a aucunement lieu à abrogation pour ce motif. L'abrogation par la voie juridictionnelle que vous avez admise, à titre subsidiaire de conclusions principales d'annulation, dans la décisions ELENA (Section, 19 novembre 2021, Association des avocats ELENA France et autres, n°s 437141, 437142, A) concerne le cas où, du fait d'un changement de circonstances de droit ou de fait, la décision en litige à caractère réglementaire est devenue illégale, si bien qu'il apparaît opportun que le juge de l'excès de pouvoir saisi d'un recours contre cet acte puisse en prononcer lui-même l'abrogation au lieu de renvoyer la partie requérante devant l'administration.

Or, la mise en demeure, qui n'est pas réglementaire du reste, ne devient pas illégale (ni même sans objet) par le fait qu'elle a été suivie d'effets. C'est sa vocation d'être suivie d'effets. A défaut d'être suivie d'effets, la procédure de sanction peut être engagée (v. article 20 III ; la mise en demeure n'est toutefois pas un préalable obligatoire à la sanction, v. 17 avril 2019, Société Optical Center, n° 422575, B ; 4 novembre 2020, Société Sergic, n° 433311, B). Mais qu'elle soit (ou non) suivie d'effets est sans incidence sur sa légalité.

B. Les autres critiques peuvent également s'écarter sans difficultés.

La présidente de la CNIL a retenu que les mots de passe que peuvent utiliser les agents ne sont pas suffisamment robustes (8 caractères dont une lettre et un chiffre), que des serveurs de la commune utilisent des systèmes d'exploitation obsolètes qui ne sont plus mis à jour (Windows 2003) et que le réseau informatique de la commune est fragile en cas d'attaques ou d'intrusions car il n'est pas segmenté. A chaque fois, la présidente de la CNIL s'est référée aux préconisations en matière de sécurité figurant dans des instruments de droit souple : une délibération de la CNIL du 21 juillet 2022 sur les mots de passe et des recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

La commune soutient que la présidente de la CNIL a ainsi commis des erreurs de droit car ces instruments n'ont pas de valeur normative et pas plus qu'ils ne sauraient fonder une sanction

(11 mars 2015, Sa Total Raffinage Marketing et Société Election Europe, n°s 368748, 368819, T. p. 683), ils ne peuvent justifier une mise en demeure. Le moyen manque cependant en fait, car la présidente n'a pas considéré que la commune avait méconnu des recommandations, mais bien qu'elle a méconnu ses obligations en matière de sécurité informatique et donc de protection des données personnelles, qui découlent du RGPD (article 32), et elle pouvait, à ce titre, comme elle l'a fait, se référer aux recommandations publiées par les autorités compétentes pour estimer que la commune avait manqué à ses obligations légales (en ce sens la décision Sa Total Raffinage Marketing et Société Election Europe, préc.). Et sur le fond, la présidente de la CNIL n'a pas commis d'erreur d'appréciation.

II. Venons-en à la vidéoprotection. La commune de Beaucaire dispose, depuis 1995, d'un système de videoprotection, autorisé par des arrêtés successifs du préfet des Bouches-du-Rhône. Ce système compte aujourd'hui 73 caméras, dont 6 permettent la lecture automatique des plaques d'immatriculation.

La videoprotection implique le traitement de données personnelles. Elle est donc soumise au RGPD et à la loi du 6 janvier 1978. L'article L. 251-1 du code de la sécurité intérieure[4], dans sa version issue la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, le rappelle[5].

En l'espèce, la présidente de la CNIL, dans la mise en demeure en litige, a considéré que la commune avait manqué à son obligation de réaliser une analyse d'impact et qu'elle mettait en œuvre un traitement de données illicite et illégitime s'agissant de la lecture automatique des plaques d'immatriculation.

A. Sur l'analyse d'impact préalable à la mise en œuvre d'un système de videoprotection.

L'analyse d'impact est prévue tant par l'article 35 du RGPD pour les traitements de données qui en relèvent[6] que par l'article 90 de la loi informatique et libertés pour les traitements qui entrent dans le champ de la directive « police-justice »[7]. Un système de videoprotection est soumis à l'un ou à l'autre selon la ou les finalités mises en œuvre, lesquelles sont listées à l'article L. 251-2 du CSI[8] : s'il est autorisé à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites matière pénale ou d'exécution de sanctions pénales, il est soumis à la directive « police-justice » ; à défaut c'est le RGPD qui s'applique[9].

---

[4] v. aussi l'article L. 255-1 du CSI.

[5] Auparavant, l'application du droit des données personnelles était envisagée en cas d'enregistrement des images, ce qui n'est pas compatible avec le RGPD.

[6] v. article 62 de la loi du 6 janvier 1978.

[7] Directive n° 2016/680 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil (article 27).

[8] En matière de sûreté de l'Etat et de défense (Titre IV de la loi du 6 janvier 1978), soit la sauvegarde des installations utiles à la défense nationale (2° du L. 251-2) et la prévention d'actes de terrorisme, il n'y a pas d'analyse d'impact.

[9] Pour la position de la CNIL, v. www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables.

Un système de videoprotection pouvant poursuivre plusieurs finalités, les deux corps de règles sont susceptibles de s'appliquer concomitamment.

En l'espèce, la videoprotection a été autorisée dans la commune de Beaucaire pour assurer la sécurité des personnes, la prévention des atteintes aux biens, la protection des bâtiments publics, la prévention du trafic de stupéfiants. La présidente de la CNIL, dans sa mise en demeure, s'est fondée sur la directive transposée dans la loi, tout en se référant au RGPD.

En vertu de ces deux textes, une analyse d'impact est nécessaire lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, apprécié compte tenu de la nature, de la portée, du contexte et des finalités du traitement, ainsi que le recours à des nouvelles technologies.

Le RGPD est un peu plus précis que la directive, car il indique, sans être limitatif, trois cas dans lesquels l'analyse d'impact est requise, dont « la surveillance systématique à grande échelle d'une zone accessible au public ».

Pour considérer qu'une analyse d'impact aurait dû être réalisée par la commune de Beaucaire, la présidente de la CNIL a retenu que la commune, d'une population de 16 000 habitants, utilise 73 caméras situées notamment aux abords de places, de la mairie et de parkings, ce qu'elle a qualifié de surveillance systématique à grande échelle de zones accessibles au public.

La commune de Beaucaire considère en premier lieu que cette partie de la mise en demeure est insuffisamment motivée. Vous pourrez écarter ce moyen.

L'exigence de motivation des mises en demeure ne résulte pas de l'article L. 211-1 du CRPA (anciennement loi du 11 juillet 1979) car la mise en demeure ne relève d'aucune des catégories de décisions prévues à cet article[10]. En revanche, elle se déduit de l'article 38 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978, qui prévoit que la mise en demeure précise le ou les manquements aux obligations incombant au responsable du traitement ou au sous-traitant et fixe le délai au terme duquel le responsable du traitement ou le sous-traitant est tenu d'avoir fait cesser le ou les manquements constatés[11].

En l'espèce, la mise en demeure, après mention des textes applicables, énonce les critères de fait sur lesquels elle s'est fondée : le nombre de caméras, le type de lieux où elles sont disposées, la population communale ; puis elle en tire une qualification légale, celle de surveillance systématique à grande échelle d'une zone accessible au public. Elle en déduit qu'une analyse d'impact était nécessaire et que la commune a donc manqué à son obligation. Cette motivation, sans être excessivement développée, est suffisante.

La commune soutient en second lieu que la présidente de la CNIL a inexactement qualifié les faits de l'espèce en considérant qu'une analyse d'impact était nécessaire. La commune engage

[10] En ce sens 10 JS, 11 avril 2014, Association Juricom et Associés, n°348111.
[11] En ce sens, 11 mars 2015, Société Tuto4PC, n° 368624, B sur un autre point.

pour ce faire une discussion essentiellement chiffrée sur le nombre de personnes potentiellement concernées par la videoprotection, tout en contestant que l'équation puisse se résoudre par le nombre de caméras rapporté au nombre d'habitants.

La commune semble vouloir dire qu'il est exagéré de retenir la population municipale, car, compte-tenu de l'emplacement des caméras, toute la population n'est pas concernée. A vrai dire, l'argument s'inverse aisément : compte-tenu de la disposition des caméras, toute personne qui se déplace dans le centre de Beaucaire ou traverse la commune selon un axe est-ouest est susceptible d'être filmée, qu'elle soit habitante de Beaucaire ou non, soit, au total, beaucoup plus que 16 000 personnes.

Mais, en tout état de cause, nous vous invitons à ne pas rentrer dans cette logique d'ordre mathématique. En effet, il ne faut pas perdre de vue que le critère de l'analyse d'impact, c'est le risque élevé pour les droits et les libertés des personnes physiques et ce risque doit s'apprécier en tenant compte de la nature, de la portée, du contexte et des finalités du traitement, ainsi que le recours à des nouvelles technologies. La surveillance systématique à grande échelle d'une zone accessible au public n'est qu'une déclinaison de ces critères d'appréciation, pour lesquels il n'y a pas lieu de faire jouer des seuils ou des ratios.

A notre sens, car c'est ainsi que nous comprenons l'expression de « surveillance systématique à grande échelle d'une zone accessible au public », un système de videoprotection implique par principe qu'une analyse d'impact soit réalisée. Les finalités du système étant la protection des personnes et des biens et la prévention des troubles et des infractions, c'est le comportement des personnes qui est visé par le système de captation d'images. Le système étant déployé en plusieurs points stratégiques de la commune (les places, les axes principaux), il est destiné à filmer un nombre important de personnes, il est donc à grande échelle sur des zones publiques. Il fonctionne en outre de manière continue, en tout cas il n'est pas ponctuel, il a donc un caractère systématique. Peu importe qu'il y ait 10 000 ou 100 000 habitants dans la commune, 25 ou 250 cameras[12], il y en a suffisamment, d'habitants comme de caméras, pour que le risque d'atteinte aux droits et libertés, que sont la liberté de circuler et le respect de la vie privée, soit élevé.

Si bien que quand une commune déploie un système de videoprotection, elle doit – c'est l'objet de l'analyse d'impact – s'interroger sur les finalités du traitement, évaluer la nécessité et la proportionnalité des opérations qu'il implique au regard de ces finalités, identifier concrètement les risques pour les droits et libertés des personnes et envisager les mesures permettant de faire face à ces risques du point de vue de la protection des données personnelles. C'est un exercice de réflexion qui se présente comme une contrainte raisonnable pour le responsable de traitement et une saine garantie pour les droits des personnes[13].

Ce n'est que par exception qu'un système de captation d'images pourra être dispensé d'analyse d'impact. Par ex. si une collectivité publique installe une seule caméra, devant un

[12] Pour un aperçu dans d'autres villes, datant de 2020, v. www.lagazettedescommunes.com/660599/le-palmares-des-50-plus-grandes-villes-videosurveillees.
[13] Et elle doit consulter l'autorité de contrôle si le niveau de risque reste élevé en dépit des mesures envisagées.

bâtiment public, pour évaluer le flux de passants et vérifier si une file d'attente est en train de se former, afin d'ajuster l'accueil. Ce n'est pas de la videoprotection, un seul lieu est concerné, ce n'est pas le comportement des personnes qui est en cause, mais une quantité de personnes, une fréquentation d'un lieu. Le risque est a priori négligeable pour les libertés.

En l'espèce, 73 caméras installées aux abords des places, de la mairie et des parkings, il y a bien un risque élevé pour les droits et libertés des personnes, résultant d'une surveillance systématique à grande échelle de zones accessibles au public et imposant la réalisation d'une analyse d'impact préalable à la mise en œuvre du traitement des données de la videoprotection (et sa mise à jour en cas d'évolution du système de videoprotection).

C'est donc sans commettre d'erreur que la présidente de la CNIL a relevé un manquement de la commune de Beaucaire et l'a mise en demeure de réaliser cette analyse d'impact.

B. Sur la licéité et la légitimité de la lecture automatique des plaques d'immatriculation.

Pour la présidente de la CNIL, la commune n'est pas habilitée à recourir à la lecture automatisée des plaques d'immatriculation et, en outre, elle l'utilise pour des finalités qui ne sont pas légitimes. La commune conteste ces deux appréciations.

La commune a raison sur le premier point. Pour la CNIL, il résulte des articles L. 233-1 et L. 233-1-1 du code de la sécurité intérieure, respectivement créés par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure et la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, que seuls les services de police, de gendarmerie nationales et des douanes peuvent mettre en œuvre des dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules.

Mais si ces deux articles prévoient en effet que la police, la gendarmerie et les douanes peuvent contrôler automatiquement les données signalétiques des véhicules afin de lutter contre la criminalité organisée, le vol de véhicules et les infractions au code de la route, et si à cette fin a été autorisé un traitement de données du contrôle automatisé des données signalétiques des véhicules, placé sous la responsabilité conjointe du directeur général de la police nationale, le directeur général de la gendarmerie nationale et le directeur général des douanes et droits indirects (arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules), ce n'est pas pour autant, comme le soutient la CNIL, qu'il s'en déduit, par a contrario, que les autres administrations ne pourraient pas mettre en œuvre un système de lecture automatisé des plaques d'immatriculation.

Elles le pourraient en effet, sur le fondement de l'article L. 251-2 du code de la sécurité intérieure, dans le cadre d'un système de videoprotection.

C'est la lecture que défendait Edouard Crépey dans ses conclusions sur votre décision Commune de Gujan-Mestras du 27 juin 2016 (n°385091, p. 256) et nous comprenons votre décision, qui n'a pas opposé à la commune qu'elle était radicalement incompétente pour

recourir à la lecture automatisée des plaques d'immatriculation, que vous avez adhéré à cette lecture du code de la sécurité intérieure.

Nous vous proposons de la confirmer explicitement dans la présente affaire, sans vous laissez impressionner par un argument supplémentaire invoqué par la CNIL dans son mémoire en défense selon lequel le code de la sécurité intérieure n'autoriserait que les systèmes de videoprotection « traditionnels », c'est-à-dire des caméras qui enregistrent des images, mais ne permettrait pas l'utilisation de systèmes de caméras « augmentées » ou « intelligentes ».

La CNIL en veut pour preuve qu'une disposition législative a été nécessaire pour permettre, à titre expérimental du reste, l'utilisation de « caméras intelligentes » pour mieux assurer la sécurité d'évènements sportifs, festifs ou culturels, particulièrement exposés à des risques, notamment de nature terroriste (article 10 de la loi précitée du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions).

Cependant, et alors qu'il n'existe pas de définition des « caméras intelligentes », il ne faut pas perdre de vue que la lecture automatisée des plaques d'immatriculation n'est, en elle-même, rien d'autre que la mise en œuvre d'un logiciel de reconnaissance de texte, qui se borne à transformer en texte des lettres et des chiffres captés au format image, comme pourrait le faire manuellement un agent derrière son écran qui noterait sur un calepin la plaque d'immatriculation du véhicule[14].

Le dispositif envisagé par le législateur en 2023 est différent. Il s'agit de soumettre les images captées par la videoprotection ou des drones à un logiciel d'intelligence artificielle destiné à détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler des risques, c'est-à-dire d'analyser les comportements des personnes filmées afin de détecter des anomalies : par ex., le traitement algorithmique va être utilisé, s'il en est capable, pour vérifier si, alors que vous marchez sur le trottoir, vous sortez de votre poche un parapluie ou une arme…

Comme l'a indiqué l'Assemblée générale du Conseil d'Etat dans son avis rendu sur le projet de loi (15 décembre 2022, n° 406383), et c'est d'ailleurs également l'opinion exprimée par la CNIL dans sa position du 19 juillet 2022 sur le déploiement de caméras « augmentées » dans les espaces publics[15], l'intervention du législateur se justifie car il s'agit de définir pour la première fois un dispositif inédit porteur d'enjeux nouveaux pour les droits et libertés, l'IA appliquée à la surveillance vidéo ne constituant pas une simple évolution technologique, mais une modification de la nature même des dispositifs vidéo.

Rien de tel avec la lecture automatique des plaques d'immatriculation. Contrairement à ce que retenu la présidente de la CNIL, une commune n'est pas exclue, par principe, de cette fonctionnalité.

[14] En revanche, la mise en relation d'une LAPI avec d'autres traitements de données peut permettre de générer des informations supplémentaires.

[15] www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position

Cependant, si l'utilisation d'un logiciel de LAPI n'est pas en soi illicite, il peut être illégitime au regard de la finalité poursuivie, c'est-à-dire qu'une commune peut recourir à la lecture automatisée des plaques d'immatriculation dans le cadre de la vidéoprotection mais pour autant que l'usage qu'elle en fait soit conforme aux finalités pour lesquelles elle a été autorisé à déployer un système de videoprotection.

Or, en l'espèce, la commune de Beaucaire a expliqué à la CNIL, et elle le soutient aussi devant vous, qu'elle collecte les numéros des plaques d'immatriculation afin de pouvoir les fournir aux services de police ou de gendarmerie en cas de réquisitions dans le cadre d'une enquête. Mais ce n'est pas une finalité prévue par l'article L. 251-2 du code la sécurité intérieure sur la vidéoprotection. C'est ce motif que vous aviez retenu dans l'affaire concernant la commune de Gujan-Mestras. Il a été opposé à bon droit à la commune de Beaucaire.

Dans ces conditions, la mise en demeure prononcée par la présidente de la CNIL, si elle est entachée d'erreur de droit sur l'illicéité de l'utilisation de la LAPI par la commune de Beaucaire, est en revanche fondée en ce qui concerne l'illégitimité de cette utilisation par la commune. Il n'y a donc pas lieu de l'annuler.

PCMC rejet de la requête.