CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

Monsieur Christian ESTROSI
Maire
MAIRIE DE NICE
5/7 PLACE DU GENERAL DE GAULLE
06000 - NICE

Paris, le 10 AVR. 2018

N/Réf. : IFP/AME/DI181074
A rappeler dans toute correspondance

Monsieur le Maire,

Le 8 janvier dernier, le Correspondant Informatique et Libertés (CIL) de la Ville de Nice a saisi la Commission nationale de l'informatique et des libertés d'une demande de conseil concernant la mise œuvre imminente d'un projet d'expérimentation de l'application mobile « Reporty ». 2 000 volontaires (agents de la Ville, de son CCAS, de la Métropole Nice Côte d'Azur, voisins-vigilants et membres des comités de quartier de la commune) s'apprêtaient alors à tester les fonctionnalités de cette application, développée par une société israélienne et dont un pilote avait été mis à disposition de votre collectivité pour une période allant du 10 janvier au 10 mars 2018.

L'outil « *connecte en temps réel les citoyens à la police municipale* » pour permettre à celle-ci d'adapter sa réponse en cas d'incidents. Il propose à ses utilisateurs la possibilité de signaler aux forces de l'ordre « *une incivilité grave (dépôt sauvage d'encombrants ou de déchets sur la voie publique, tags conséquents sur un bien public) ou une « situation critique » (actes de violence, vol, enlèvement, attentat, effondrement, inondation, incendie, accident)* » dont ils seraient témoins ou victimes, en transmettant en direct au Centre de Supervision Urbain (CSU), où sont par ailleurs diffusés les enregistrements visuels issus des systèmes de vidéoprotection, leur localisation géographique ainsi qu'une vidéo – image et son – de leur environnement immédiat et des évènements en cours.

Aux fins d'éviter les abus au stade de l'exploitation de l'application, la collectivité a conditionné celle-ci à une inscription préalable, au suivi en présentiel d'un tutoriel de présentation, ainsi qu'à la signature d'une charte d'utilisation. Aux termes de cette charte, les utilisateurs s'engagent notamment, sous peine d'une désinscription automatique, à ne pas filmer des lieux privés, à ne capter que des faits en cours de réalisation et présentant un caractère de gravité ou d'urgence, à faire preuve de discernement dans la perception des faits dont ils seront témoins, à ne pas perturber le bon fonctionnement de la police municipale et à ne pas y recourir pour se venger d'autrui par rapport à une situation personnelle.

Mi-février, le CIL de la Ville de Nice nous indiquait que s'il était initialement prévu que le CSU enregistre l'ensemble des flux qui lui parviennent, il avait finalement été décidé que les données audiovisuelles seraient gérées exclusivement en temps réel par ses opérateurs ; que pour autant, les observations de notre Commission devaient tenir compte du souhait de la collectivité de procéder à un enregistrement des flux audiovisuels pour une utilisation à des fins probatoires, dans l'hypothèse où l'expérimentation, désormais en cours de mise en œuvre, se révélait concluante et que le dispositif aurait alors vocation à être pérennisé.

A titre liminaire, je ne peux que regretter que notre Commission n'ait pas été saisie davantage en amont du déclenchement de l'expérimentation, celle-ci portant sur un dispositif de signalement faisant un usage nouveau des technologies existantes et appelant, de toute évidence, une vigilance particulière du fait de l'importance des risques potentiels pour la vie privée et les libertés publiques. Ces risques ont d'ailleurs été parfaitement identifiés par la Ville elle-même, puisqu'elle y consacre le point III de sa charte d'utilisation précédemment évoquée.

Le dispositif en question ayant fait l'objet d'un débat collégial des membres de la Commission lors de la séance plénière du 15 mars dernier, je suis en mesure de vous faire part des éléments d'analyse suivants, que vous trouverez également développés dans la note jointe à ce courrier.

En premier lieu, la Commission estime que cet outil, dont la mise en œuvre repose sur la collecte et l'enregistrement d'images et de sons par la police municipale intervenant dans l'exercice de sa mission de sauvegarde de l'ordre public, devrait faire l'objet d'un encadrement législatif spécifique, à l'instar de ce qui existe actuellement pour d'autres dispositifs, sinon identiques, du moins comparables, de vidéoprotection.

A cet égard, je vous rappelle que la CNIL a retenu une telle analyse en 2015 s'agissant du recours à des caméras mobiles par les forces de l'ordre pour prévenir la commission d'infractions lors de leurs interventions, en déterminer les circonstances et disposer d'enregistrements audiovisuels à des fins probatoires. En effet, la collecte et l'enregistrement d'images par les autorités publiques, pour des finalités de maintien de l'ordre et de la sécurité publics, faisaient déjà l'objet d'un encadrement juridique spécial et strict (Livre II du Code de la sécurité intérieure/CSI, Titres II à V), notamment pour que soient limitées les atteintes aux droits et libertés fondamentaux susceptibles d'en résulter. Compte tenu des problématiques particulières soulevées par l'exploitation de ces nouveaux outils et des risques accrus pour les libertés et la vie privée des personnes (enregistrements sonores et captation d'images dans des lieux privés, en particulier), la CNIL a estimé qu'ils devaient faire l'objet d'un encadrement par le législateur. Ainsi, le CSI a été enrichi de nouvelles dispositions en ce sens, avec la loi n°2016-73 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.

Au regard de ce qui précède, il apparaît que la mise en œuvre de dispositifs tels que « Reporty », qui impliquent l'intervention d'un très grand nombre de personnes privées dans la collecte d'images et de sons sur la voie publique, et qui emportent *de facto* une extension des systèmes de vidéoprotection de la Ville ainsi que de ses capacités de collecte de flux audiovisuels à partir de caméras mobiles, doit nécessairement se fonder sur une base légale solide, d'un niveau juridique équivalent et de nature à apporter les garanties nécessaires à la préservation des droits et libertés fondamentaux.

En deuxième lieu, la Commission, sans évidemment remettre en cause la légitimité de la finalité poursuivie par le dispositif, à savoir la sécurité publique, a relevé que ses caractéristiques de mise en œuvre, tel qu'expérimentées et envisagées sur le long terme par la collectivité, n'apparaissaient pas de nature à garantir le respect des principes protecteurs des données personnelles, en particulier celui ayant trait à la proportionnalité des traitements effectués.

En effet, la mise à disposition de l'application couvre un champ extrêmement large d'incidents, allant d'incivilités jusqu'à des infractions délictuelles et criminelles graves. Elle conduit par ailleurs nécessairement à une collecte, par nature intrusive, d'une grande volumétrie d'images et de sons tirés de l'environnement des utilisateurs, sans que la nature des données captées, et donc leur caractère strictement nécessaire à l'objectif poursuivi, puisse en amont être filtré par la collectivité ; sans également que les personnes concernées par ses captations (personnes visées et tiers présents sur la voie publique) puissent être informées de la réalisation de ces dernières au moment où elles surviennent.

Par ailleurs, les garanties prévues par la collectivité, en particulier la charte de bonnes pratiques susceptible de conduire à la simple désinscription du service en cas de mésusage, n'apparaissent pas suffisantes compte tenu de l'ampleur et de la portée du dispositif rappelée ci-dessus.

En conclusion, je vous informe que compte tenu de l'ensemble des éléments qui précèdent, la Commission estime que la pérennisation du dispositif, tout comme le projet de poursuite de son expérimentation jusqu'au 30 avril dont votre CIL vient de faire part à mes services, se heurtent aujourd'hui à d'importantes difficultés. La CNIL a d'ailleurs l'intention d'alerter le ministère de l'Intérieur sur les problématiques en cause, et en particulier celle liée à la fragilité de la base légale de ce type de dispositifs.

Tel sont les éléments de fond justifiant la position prise par la Commission que je tenais à porter à votre connaissance sur cette problématique qui se prête malaisément à des propos inutilement simplificateurs et polémiques.

Mes services restant à votre disposition pour toute information complémentaire, je vous prie d'agréer, Monsieur le Maire, l'assurance de mes salutations distinguées.

Isabelle FALQUE-PIERROTIN

DEVELOPPEMENT DES ELEMENTS D'ANALYSE DE LA COMMISSION

I. SUR LA FRAGILITE DE LA BASE LEGALE DE CE TYPE DE DISPOSITIF EN L'ETAT ACTUEL DU DROIT

En premier lieu, la Commission a observé que la collecte et l'enregistrement d'images et de sons par les autorités publiques, pour des finalités de maintien de l'ordre et de la sécurité publics, font l'objet d'un encadrement juridique spécial et strict, de nature législative (Livre II du Code de la sécurité intérieure/CSI, Titres II à V), notamment pour que soient limitées les atteintes aux droits et libertés fondamentaux susceptibles d'en résulter.

Le CSI (art. L. 251-1 et suiv.) encadre ainsi la mise en œuvre de dispositifs de vidéoprotection sur la voie publique, en précisant :

- les finalités limitatives auxquelles ils peuvent répondre (prévention des actes de terrorisme, des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants, constatation des infractions aux règles de la circulation, secours aux personnes et défense contre l'incendie, etc.),
- leurs caractéristiques de fonctionnement (notamment la détermination des lieux d'implantation et l'orientation des caméras, les conditions d'accès et de transmission des images aux services de police et de gendarmerie nationales, des douanes et des services d'incendie et de secours, ainsi que leur durée de conservation),
- les garanties pour les personnes dont ils doivent être assortis (pas de visualisation de l'intérieur et des entrées des immeubles d'habitation, information du public sur l'existence et la localisation de ces systèmes, droit d'accès des intéressés aux enregistrements visuels, etc.),
- et les modalités de contrôle de ces dispositifs (autorisation préfectorale prise après avis d'une commission départementale de vidéoprotection et contrôle a posteriori de la CNIL).

Le CSI (art. L. 272-1) renvoie également à des dispositions du Code de la construction et de l'habitation (art. L. 126-1-1) pour ce qui est des conditions dans lesquelles des images collectées par des dispositifs implantés dans les parties communes d'immeubles d'habitation peuvent être transmises aux services chargés du maintien de l'ordre :

- décision de la majorité des copropriétaires et, dans les immeubles sociaux, du gestionnaire ; nécessité de circonstances faisant redouter la commission imminente d'une atteinte grave aux biens ou aux personnes ;
- transmission en temps réel et strictement limitée à l'intervention des forces de l'ordre nationales ou locales ;
- convention préalable entre le(s) gestionnaire(s) de l'immeuble et le représentant de l'Etat dans le département précisant les conditions et modalités du transfert et transmise à la commission départementale de vidéoprotection à des fins d'appréciation de la pertinence des garanties prévues.

Enfin, à la demande de la Commission, au regard des problématiques particulières soulevées par leur exploitation et des risques accrus pour les droits et libertés des personnes (enregistrements sonores et captation d'images dans des lieux privés, en particulier), le CSI a récemment été enrichi de dispositions législatives encadrant spécifiquement le recours à des caméras mobiles par les forces de l'ordre, pour prévenir la commission d'infractions lors de leurs interventions, en déterminer les circonstances et disposer d'enregistrements audiovisuels à des fins probatoires :

- dans sa délibération n°2015-253, la CNIL a en effet indiqué que « *les conditions de mise en œuvre des dispositifs projetés diffèrent largement de celles concernant les dispositifs fixes dits*

de « vidéoprotection », qui sont strictement encadrés par les dispositions législatives du code de la sécurité intérieure. De même, ces conditions sont distinctes de celles habituellement applicables aux dispositifs de « vidéosurveillance » régis par la loi du 6 janvier 1978 modifiée. Dès lors, et au regard des risques élevés de surveillance des personnes et d'atteinte à la vie privée qui pourraient résulter d'un usage non maîtrisé de caméras mobiles, la Commission considère que ces dispositifs devraient faire l'objet d'un encadrement législatif spécifique » ;

- ainsi, la loi n°2016-731 a ouvert la possibilité d'utiliser des caméras-piétons aux agents de la police et de la gendarmerie nationales ainsi que, à titre expérimental, à ceux de la police municipale (art. L241-1 du Code de la sécurité intérieure). Ce texte et ses décrets d'application (n°2016-1860 et n°2016-1861) ont assorti l'utilisation de ces outils de garanties spéciales, notamment l'exclusion des caméras/smartphones personnels des agents (recours à l'équipement professionnel), l'absence d'enregistrement permanent des interventions, l'information des personnes concernées lors de l'enregistrement, l'interdiction de consulter les images indépendamment d'une procédure judiciaire, administrative ou disciplinaire ou d'une action de formation et de pédagogie des personnels.

En deuxième lieu, la Commission a relevé que les dispositifs tels que « Reporty » emportent *de facto* une extension des systèmes de vidéoprotection de la Ville, ainsi qu'une extension de ses capacités de collecte de flux audiovisuels à partir de caméras mobiles en dehors de tout cadre prévu par le CSI ; que « Reporty » va en outre bien au-delà de ces dispositifs en impliquant notamment l'intervention d'un très grand nombre de personnes privées dans la collecte d'images et de sons et, ce faisant, une multiplication des risques d'atteintes à la vie privée et aux libertés des individus.

Au regard de l'ensemble de ces éléments, et sans se prononcer sur le principe général des dispositifs de « vigilance citoyenne », la Commission a estimé que la a mise en œuvre de l'application « REPORTY» s'inscrit en effet difficilement dans le cadre légal actuel fixé par le CSI et qu'un cadre juridique spécifique, d'un niveau normatif équivalent à celui sur lesquels s'appuient les dispositifs précédemment évoqués semblait s'imposer pour apporter les garanties nécessaires à la préservation des droits et libertés fondamentaux.

II. SUR LES PROBLEMATIQUES SOULEVEES PAR LE DISPOSITIF EN QUESTION AU REGARD DU CADRE JURIDIQUE DE LA PROTECTION DES DONNEES PERSONNELLES

Sans remettre en cause la légitimité de la finalité poursuivie, la Commission a relevé, au terme d'un examen circonstancié des caractéristiques de mise en œuvre du traitement, tel qu'expérimentées et envisagées sur le long terme par la collectivité, que le dispositif était susceptible de porter atteinte aux principes protecteurs des données personnelles.

En particulier, s'agissant d'un dispositif mis en œuvre pour des motifs d'ordre et de sécurité publics, un équilibre doit être assuré entre les atteintes aux droits et libertés pouvant en résulter et les garanties mises à place par l'autorité compétente pour limiter de telles atteintes,

Dans un premier temps, la Commission s'est ainsi livrée à une analyse de la proportionnalité du traitement en cause, qui l'a conduite à relever les éléments suivants :

- la définition par la charte des cas d'utilisation de l'application est extrêmement large (dépôts sauvages d'encombrants et de déchets sur la voie publique) pour permettre par exemple la captation de l'image et de l'environnement sonore d'une personne laissant un objet sur le trottoir le temps d'aller chercher sa voiture pour le récupérer, ou encore d'une personne jetant dans le caniveau un mégot de cigarette ou ne ramassant pas les déjections de son chien sur la voie publique ; or, si l'article R633-6 du Code pénal incrimine expressément de tels comportements, leur niveau de « gravité » très variable ne saurait que très difficilement justifier dans tous les cas

de figure de potentielles atteintes à la vie privée des personnes entrant dans le champ de la caméra et du microphone de l'utilisateur de l'application ;

- les dispositifs de captation d'images et de sons sont en eux-mêmes particulièrement intrusifs en ce qu'ils fournissent de nombreuses informations sur les personnes intéressées, telles que leur présence et leur comportement en un endroit et à un moment donnés, ainsi que la teneur d'éventuelles conversations privées ; ainsi, la CNIL fait preuve d'une grande vigilance quant à la proportionnalité des systèmes de vidéosurveillance et se montre traditionnellement très réservée sur le couplage de ceux-ci à des mécanismes d'enregistrement sonore (jugés par principe comme étant excessifs) ; de même, comme vu précédemment, le CSI encadre strictement le recours à ces dispositifs, qu'ils soient exploités isolément ou cumulativement (ses dispositions sur les systèmes de vidéoprotection ne permettent pas l'enregistrement du son, tandis que celles qui l'autorisent pour les caméras mobiles se fondent sur la nature particulière des circonstances dans lequel cet enregistrement intervient et ne permettent la consultation des données qu'*a posteriori* et dans des cas limités) ;

- nonobstant la simple obligation de signature d'une charte d'utilisation avant l'exploitation de l'application, sanctionnée par la seule désinscription éventuelle de l'utilisateur en cas de mésusage ou d'abus, la mise à disposition de celle-ci incitera *de facto* les particuliers à multiplier les captations d'images et de sons tirés de leur environnement, sans que le champ des données captées, et *a fortiori* leur caractère strictement nécessaire à l'objectif poursuivi, puisse en amont être filtré par la collectivité ; sera ainsi collecté, voire enregistré, un volume important de données personnelles sans lien direct avec les incidents (passants/témoins non impliqués dans les évènements visés), ou sans rapport réel avec la commission d'une infraction/d'une « grave incivilité» (erreurs d'appréciation/présomptions d'utilisateurs potentiellement fondées sur des préjugés discriminatoires), ou encore sans objet au regard des missions de la police municipale ou sans respect des termes de la charte (ex. : utilisation de l'outil dans le cadre de règlements de compte personnels ou dans des lieux privés) ;

- par ailleurs, la Ville de Nice dispose déjà d'un certain nombre de dispositifs visant à la sécuriser, à mettre un terme aux troubles à l'ordre public et à faire participer ses citoyens à la sauvegarde de celui-ci ; tels que l'appel à la police municipale, au « 17 » ou au « 112» (saisines des services de police nationale et de secours), ou encore de l'utilisation du dispositif « Allo Mairies » (par exemple, pour le nettoyage d'un tag sur un bien public) ;

- de plus, indépendamment du recours à une telle application, qui par son existence même favorisera la pratique de signalement, les citoyens pourront toujours transmettre aux forces de l'ordre des enregistrements audiovisuels de situations « inquiétantes » dont ils auront été témoins ou victimes, bien qu'en différé ;

- enfin, un tel dispositif comporte des risques d'atteinte à la sécurité des utilisateurs de l'application, comme à celle des personnes se trouvant réellement dans une situation de danger ; en effet, certains utilisateurs pourraient s'exposer dangereusement pour dénoncer un incident, tandis que des personnes victimes d'infractions pourraient voir leur situation noyée dans les flux d'images, sons et appels alors transmis au service de police municipale.

Compte tenu de l'ensemble de ces éléments, la Commission a estimé que ce dispositif n'apparaissait pas conforme à l'exigence de proportionnalité des traitements mis en œuvre, en ce qu'il emportait des risques particulièrement importants de surveillance incontrôlée et d'atteintes à la vie privée des administrés, sans que les garanties l'entourant soient suffisantes pour cantonner ces risques à un niveau acceptable.

Dans un second temps, la Commission s'est attachée à évaluer les conditions de mise en œuvre du dispositif au regard du principe suivant lequel les traitements de telles données devaient être effectués « *de manière loyale* » (art. 6 de la loi « Informatique et Libertés » et articles 12 du RGPD et de la

directive « police-justice » qui posent un principe général de transparence et de facilitation de l'exercice des droits).

A cet égard, elle a souligné que l'utilisation de l'application « Reporty », qui vise à attirer discrètement l'attention des forces de l'ordre, ne saurait répondre à une exigence d'information individuelle – seule une information générale sur le site internet de la collectivité ou par voie d'affichage peut être réalisée – et emporte ainsi en pratique la collecte d'images et de sons à l'insu des personnes concernées.

Or, si le cadre juridique de la protection des données personnelles prévoit des dérogations à l'obligation d'information des personnes concernées – en particulier lorsqu'une telle information ferait obstacle à la satisfaction des objectifs poursuivis en matière de prévention, de recherche, de constatation ou de poursuite d'infractions pénales (art. 32 de la loi, art. 13 de la directive), la Commission, dans son avis de 2015 sur le projet de décret autorisant le port de caméras individuelles par les agents de la police et de la gendarmerie nationale, a indiqué qu'« *une telle information, obligatoire en matière de vidéo, constitue une garantie essentielle* » en ce qu'elle est « *de nature à assurer une meilleure proportionnalité des traitements projetés* », ainsi que l'effectivité du droit d'accès des intéressés. Le législateur a rejoint cette analyse puisqu'aux termes de l'article L. 241-1 du CSI, outre l'information générale livrée au public via leurs sites institutionnels, les autorités publiques devront veiller à ce que les caméras soient « *portées de* façon *apparente* » par leurs agents habilités et qu' « *un signal visuel spécifique indique si la caméra enregistre* ». Le déclenchement de l'enregistrement doit de surcroît faire l'objet d'une information des personnes filmées, sauf si les circonstances l'interdisent.

Ces considérations renforcent le besoin d'un encadrement légal spécifique de ces dispositifs.

En conclusion, au regard des risques élevés de surveillance des personnes et d'atteinte à la vie privée qui pourraient résulter d'un usage non maîtrisé d'un tel dispositif, la Commission a considéré qu'il était hautement souhaitable que sa mise en œuvre puisse s'appuyer sur un fondement législatif spécifique et qu'en tout état de cause, sa proportionnalité n'était en l'état pas garantie.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Communication présentée en séance plénière le 15 mars 2018

COMMUNICATION RELATIVE AUX CONDITIONS DE MISE A DISPOSITION DES ADMINISTRES D'UNE APPLICATION MOBILE PERMETTANT DE SIGNALER DES INCIDENTS AU SERVICE DE POLICE MUNICIPALE, VIA LA TRANSMISSION EN TEMPS REEL DE VIDEOS (PROJET « REPORTY » DE LA VILLE DE NICE)

Rapporteur : M. **Jean-François CARREZ**

Avec le concours de :
Mme Alice de LA MURE
Juriste au Service des Correspondants Informatique et Libertés

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Résumé / synthèse de la position de la CNIL

Par l'intermédiaire de son correspondant « informatique et libertés » (CIL), la Ville de Nice a saisi début janvier les services de la CNIL d'une demande de conseil concernant la mise œuvre imminente d'un projet d'expérimentation de l'application mobile « Reporty », développée en Israël par la start-up de l'ancien premier ministre et ministre de la Défense Ehud Barak.

Cette application, dont un pilote a été mis à disposition de la Ville pour une période de deux mois, **« *connecte en temps réel les citoyens à la police municipale* », pour permettre à celle-ci d'intervenir aussi rapidement qu'efficacement en cas d'incidents**. Visant à « *faire de chacun un citoyen engagé acteur de sa propre sécurité, et donc de la sécurité collective* » (C. Estrosi), **l'outil offre ainsi à ses utilisateurs la possibilité de signaler à la police « *une incivilité grave* *(dépôt sauvage d'encombrants ou de déchets sur la voie publique, tags conséquents sur un bien public)* » *ou une « situation critique »* *(actes de violence, vol, enlèvement, attentat, effondrement, inondation, incendie, accident)* »** dont ils seraient témoins ou victimes, **en transmettant en direct au Centre de Supervision Urbain (CSU) leur localisation géographique, ainsi qu'une vidéo – image et son – de leur environnement immédiat et des évènements en cours** (ou un « tchat » en mode texte, lorsque la qualité du réseau n'est pas bonne, ou un appel téléphonique).

Mis en œuvre entre début février et début mars, ce projet d'expérimentation a été largement relayé par différents médias locaux et nationaux. Il a occasionné la constitution d'un « collectif Anti-Reporty », rassemblant des personnalités du monde politique et associatif qui ont dénoncé une atteinte grave à la vie privée et aux libertés publiques.

L'expérimentation étant achevée au jour de sa présentation en séance, et conformément à la demande de la collectivité, il appartient à la Commission d'examiner les conditions dans lesquelles le dispositif aura été testé et de se prononcer sur celles qui sont envisagées pour son éventuelle pérennisation.

Cette communication s'attache à exposer les difficultés juridiques majeures auxquelles paraît se heurter le déploiement d'un tel dispositif : outre le fait que sa légalité même pourrait être remise en cause au regard des dispositions du Code de la sécurité intérieure, il ne semble pas de nature à permettre le respect des principes protecteurs des données personnelles, en particulier celui ayant trait à la proportionnalité des traitements mis en œuvre.

I. Eléments de contexte

A. La saisine de la CIL de la Ville de Nice concernant l'expérimentation de l'application « REPORTY »

La CIL de la Ville de Nice nous a saisis le 8 janvier d'une demande de conseil concernant la mise œuvre imminente d'un projet d'expérimentation de l'application mobile « Reporty », développée en Israël par la start-up de l'ancien premier ministre et ministre de la Défense Ehud Barak.

Cette application, dont un pilote a été mis à disposition de la Ville pour une période allant du 10 janvier au 10 mars, **« *connecte en temps réel les citoyens à la police municipale* », pour permettre à celle-ci d'intervenir aussi rapidement qu'efficacement en cas d'incidents**. Visant à « *faire de chacun un citoyen engagé acteur de sa propre sécurité, et donc de la sécurité collective* » (C. Estrosi), **l'outil offre ainsi à ses utilisateurs la possibilité de signaler à la police « *une incivilité grave* *(dépôt sauvage d'encombrants ou de déchets sur la voie publique, tags conséquents sur un bien public)* » *ou une « situation critique »* *(actes de violence, vol, enlèvement, attentat, effondrement, inondation, incendie, accident)* »** dont ils seraient témoins ou victimes, **en transmettant en direct au Centre de Supervision Urbain (CSU) leur localisation géographique, ainsi qu'une vidéo – image et son – de leur environnement immédiat et des évènements en cours**, ou un « tchat » en mode texte (lorsque la qualité du réseau n'est pas bonne) ou un appel téléphonique.

La collectivité a souhaité tester ses fonctionnalités pour évaluer l'intérêt qu'elle présente, en tant qu'outil complémentaire à ce qui existe déjà en matière de signalement auprès des services compétents : standard téléphonique de la police municipale et service « Allo-Mairie » permettant de déclencher l'intervention de services techniques pour la résolution d'anomalies rencontrées en matière de propreté, de déchets, de voirie, d'éclairage et d'assainissement.

Elle a conditionné l'utilisation de ce nouveau service au respect de plusieurs étapes : inscription préalable de l'utilisateur avant le téléchargement de l'application (nom, prénom, numéro de téléphone obligatoires / photographie facultative), aux fins d'éviter les abus éventuels au stade de l'exploitation, ceux-ci étant sanctionnés par une désinscription automatique (appréciation au cas par cas du respect des conditions d'utilisation telles que précisées dans la charte évoquée ci-après et figurant en annexe) ; suivi en présentiel d'un tutoriel de présentation de cette application ; signature d'une charte d'utilisation, l'utilisateur s'engageant notamment à ne pas filmer des lieux privés et à ne capter que des faits en cours de réalisation et présentant un caractère de gravité ou d'urgence ; activation de l'application par la saisie d'un code personnel adressé par SMS.

Lorsque l'utilisateur utilise le service, la connexion s'effectue automatiquement avec le CSU (connexions chiffrées), service de la direction de la Police municipale : les images et sons captés ne sont pas enregistrés sur le smartphone de l'utilisateur mais diffusés

en temps réel sur les écrans dudit centre, où sont également visionnées les images issues des dispositifs de vidéoprotection de la collectivité.

Pour chaque connexion, les données d'identification de l'utilisateur, la date, l'heure, le temps, le lieu de l'appel ainsi que le tchat le cas échéant, sont conservés pendant douze jours au CSU. **S'il était initialement prévu que le CSU enregistre l'ensemble des flux qui lui parviennent, il a finalement été décidé que les données audiovisuelles seraient gérées exclusivement en temps réel par ses opérateurs, du moins le temps de l'expérimentation.**

Pour autant, dans la mesure où ce temps de l'expérimentation est désormais achevé, et comme demandé dès l'origine par la CIL, **les observations de la CNIL devront tenir compte du souhait de la collectivité de procéder à terme, c'est-à-dire dans l'hypothèse où l'expérimentation se révélait concluante et que le dispositif aurait alors vocation à être pérennisé, à un enregistrement des flux audiovisuels et conversations téléphoniques pour une utilisation à des fins probatoires** (l'ensemble de ces données serait alors conservé pendant un délai de dix jours au CSU et serait accessible au personnel habilité de la police municipale et de la DSI de la collectivité).

B. Une attente importante quant au positionnement de la CNIL sur le dispositif

Si début janvier 2 000 personnes (agents de la Ville de Nice, de la Métropole Nice Côte d'Azur et du CCAS de Nice ; voisins-vigilants et membres des comités de quartier de la commune de Nice) s'étaient portées volontaires pour tester l'application mobile, la Ville aurait retardé pendant près d'un mois la mise en œuvre de l'expérimentation, dans l'attente des observations de la Commission départementale de la vidéoprotection saisie le 12 janvier et de celles de la CNIL.

Elle a en effet dû faire face à une **pression médiatique extrêmement importante**, comme en a témoigné la veille presse du service Communication de notre Commission (articles parus notamment dans Le Monde, Le Figaro et Libération : « *A Nice, un citoyen peut devenir une caméra de surveillance* »), ainsi que les sollicitations nombreuses et diverses de journalistes dont ce dernier a fait l'objet (France 2 en particulier). En outre, autour d'un membre de l'opposition au sein du conseil municipal de Nice, une **coalition « anti-Reporty »** s'est formée courant janvier ; elle réunit divers partis politiques (PS, EELV, Insoumis, PCF, etc.) et associations (CGT, Tous citoyens, Mouvement contre le racisme, Ligue des droits de l'homme, etc.) et a annoncé son **intention de nous saisir ainsi que le Défenseur des droits** pour mettre un frein à « *la dérive sécuritaire* » et à « *l'organisation d'un processus de délation généralisée et une atteinte grave à la vie privée* ».

D'après les dernières informations fournies par la CIL aux services de la CNIL (fin février), **l'expérimentation aurait donc néanmoins commencé début février pour s'achever, comme prévu initialement, le 10 mars**. En effet, la Ville n'avait obtenu de la société israélienne la mise à disposition d'un pilote que pour une durée maximum de deux mois, à compter du 10 janvier 2018.

Dans ce contexte, **la Commission ne peut que regretter de ne pas avoir été saisie davantage en amont de la mise en œuvre du projet**. En outre, **ses observations sur le dispositif sont particulièrement attendues et devraient être largement relayées**. Votre rapporteur souhaite ainsi recueillir le point de vue des membres de la CNIL sur ses premiers éléments d'analyse, qui devraient permettre de répondre à la demande de conseil de la CIL de la collectivité, intégrant les conditions envisagées pour une éventuelle pérennisation du dispositif (enregistrement des images et des sons à des fins probatoires), ainsi qu'aux autres demandes passées et à venir, portant directement sur l'application « Reporty » ou ayant trait à des dispositifs s'en rapprochant.

Eléments d'analyse proposés par votre rapporteur

A titre liminaire, votre rapporteur tient à souligner les éléments suivants :

- le dispositif en cause ne saurait être considéré comme ayant pour objet la mise en œuvre de traitements à des fins personnelles/domestiques, dès lors qu'il organise une collecte de données pour le compte de la Ville de Nice, pour des finalités et dans des conditions déterminées par cette dernière ; ainsi, la circonstance que cette collecte fonctionne sur la base d'initiatives individuelles de particuliers apparaît sans incidence à cet égard, dès lors qu'il s'agit bien d'un dispositif institutionnel placé sous la responsabilité de la collectivité ;

- les missions, très larges, de sauvegarde de l'ordre public assignées à la police municipale, couplées au besoin exprimé par un certain nombre de niçois de bénéficier d'une plus grande réactivité et efficacité des services compétents en matière de sécurité et d'incivilités, peuvent justifier la mise à disposition des administrés d'outils de signalement d'incidents aux agents habilités ; mais de toute évidence, les modalités de mise en œuvre de tels dispositifs appellent une très grande vigilance en raison de l'importance des risques potentiels pour les libertés publiques ; or, le dispositif tel qu'envisagé semble se heurter à des difficultés de plusieurs ordres, ci-dessous exposées.

A. La question de la base légale du dispositif

Le dispositif « Reporty » est un outil qui serait mis en œuvre par une police municipale dans le cadre de sa mission de sauvegarde de l'ordre public (prévention et surveillance du bon ordre, de la tranquillité, de la sécurité et de la salubrité publiques), et qui tendrait à collecter et enregistrer des images et des sons issus de la voie publique ou de lieux ouverts au public. Votre rapporteur pose dès lors la question de savoir si ce dernier ne doit pas trouver une base légale spécifique dans les dispositions du Code de la sécurité intérieure, comme c'est le cas pour des situations sinon identiques, du moins comparables.

En effet, la collecte et l'enregistrement d'images par les autorités publiques, pour des finalités de maintien de l'ordre et de la sécurité publics, fait l'objet d'un encadrement juridique spécial et strict, de nature législative (Livre II du Code de la sécurité intérieure, Titres II à V), **notamment**

pour que soient limitées les atteintes aux libertés et droits fondamentaux (droit au respect de la vie privée en particulier) susceptibles d'en résulter :

- le CSI (art. L251-1 et suiv.) règlemente ainsi la mise en œuvre de **dispositifs de vidéoprotection sur la voie publique**, en précisant
  - les finalités auxquelles ils peuvent répondre (prévention des actes de terrorisme, des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants, constatation des infractions aux règles de la circulation, secours aux personnes et défense contre l'incendie, etc.),
  - leurs caractéristiques de fonctionnement (notamment la détermination des lieux d'implantation et l'orientation des caméras, les conditions d'accès et de transmission des images aux services de police et de gendarmerie nationales, des douanes et des services d'incendie et de secours, ainsi que leur durée de conservation),
  - les garanties pour les personnes dont ils doivent être assortis (pas de visualisation de l'intérieur ni, de façon spécifique, des entrées des immeubles d'habitation, information du public sur l'existence et la localisation de ces systèmes, droit d'accès des intéressés aux enregistrements visuels),
  - et les modalités de contrôle de ces dispositifs (autorisation préfectorale prise après avis d'une commission départementale de vidéoprotection et contrôle *a posteriori* de la CNIL) ;
- le CSI (art. L272-1) renvoie également à des dispositions du Code de la construction et de l'habitation (art. L126-1-1) s'agissant des conditions dans lesquelles des images collectées par des **dispositifs implantés dans les parties communes d'immeubles d'habitation** peuvent être transmises aux services chargés du maintien de l'ordre
  - décision de la majorité des copropriétaires et, dans les immeubles sociaux, du gestionnaire,
  - nécessité de circonstances faisant redouter la commission imminente d'une atteinte grave aux biens ou aux personnes,
  - transmission en temps réel et strictement limitée à l'intervention des forces de l'ordre nationales ou locales,
  - convention préalable entre le(s) gestionnaire(s) de l'immeuble et le représentant de l'Etat dans le département précisant les conditions et modalités du transfert et transmise à la commission départementale de vidéoprotection à des fins d'appréciation de la pertinence des garanties prévues ;

- enfin, à la demande de la CNIL (délibération n°2015-253), le CSI a récemment été enrichi de dispositions législatives encadrant spécifiquement le **recours à des caméras mobiles par les forces de l'ordre**, visant à prévenir la commission d'infractions lors de leurs interventions, à en déterminer les circonstances et à disposer d'enregistrements audiovisuels à des fins probatoires ; dans son avis sur un projet de décret autorisant de tels dispositifs par les agents de la police et de la gendarmerie nationales, la CNIL avait en effet souligné que l'exploitation de ceux-ci par les autorités publiques soulevaient des problématiques particulières et un risque accru pour les droits et libertés des personnes (en particulier, du fait des enregistrements sonores et de la captation d'images dans des lieux privés – cf. le rapport d'activité de la CNIL pour l'année 2015) ;

    - ainsi, la loi n°2016-731 a ouvert la possibilité d'utiliser des caméras-piétons aux agents de la police et de la gendarmerie nationales ainsi que, à titre expérimental, à ceux de la police municipale (art. L241-1 du Code de la sécurité intérieure) ;

    - ce texte et ses décrets d'application (n°2016-1860 et 2016-1861), pris après avis de la CNIL, ont assorti l'utilisation de ces outils de garanties particulières, notamment l'exclusion des caméras/smartphones personnels des agents (recours à l'équipement professionnel), l'absence d'enregistrement permanent des interventions, l'information des personnes concernées lors de l'enregistrement, l'interdiction de consulter les images indépendamment d'une procédure judiciaire, administrative ou disciplinaire ou d'une action de formation et de pédagogie des personnels ;

Or, « Reporty » va bien au-delà de ces dispositifs, en ce qu'il implique en particulier l'intervention d'un très grand nombre de personnes privées dans la collecte d'images et de sons. Votre rapporteur estime qu'il est problématique qu'un tel outil puisse être mis en œuvre sans être encadré par des règles de droit au moins aussi strictes que celles existant pour les outils précités.

Ainsi, il pourrait être considéré que le dispositif en cause emporte *de facto* une extension des systèmes de vidéoprotection de la Ville (transmission et enregistrement des images au CSU, au même titre que celles provenant desdits systèmes), ainsi qu'une extension de ses capacités de collecte de flux audiovisuels à partir de caméras mobiles en dehors de tout cadre prévu par le CSI ; qu'il se trouve dès lors dépourvu de base légale.

En outre, même si la police ne se « dépossède » pas, à proprement parler, de sa mission de surveillance générale de la voie publique (elle ne fait qu'« ajouter » à ses propres moyens ceux des citoyens), la question se pose de savoir si un tel dispositif ne pourrait pas se heurter à une jurisprudence constante du Conseil constitutionnel considérant

qu'est contraire à la Constitution la délégation par la loi à des personnes privées de fonctions régaliennes[1].

A l'inverse, la Ville pourrait faire valoir que la prise en considération de certaines circonstances – en particulier, le fait que le dispositif en cause a vocation à ne fonctionner que sur la base d'initiatives de particuliers, ponctuelles et isolées – permet d'estimer qu'un tel dispositif ne se heurte pas aux difficultés précédemment exposées ; qu'il pourrait dès lors être légalement mis en œuvre sans encadrement législatif spécifique, sur le fondement de l'article 7-e) de la loi « Informatique et Libertés » / article 6-1-e) du RGPD : « *traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* » (l'enregistrement des données relatives aux utilisateurs de l'application serait pour sa part fondé sur leur consentement explicite - article 6-1-a) du RGPD).

A cet égard, la CIL de la collectivité a tenu à souligner auprès des services de la CNIL qu'en pratique, le service de police municipale reçoit déjà des enregistrements audiovisuels de la part des administrés, parfois transmis via des réseaux sociaux ou d'autres dispositifs accessibles par tous sur internet, et que l'application en cause présente l'avantage d'encadrer les conditions de la collecte de ce type de données : notamment, les flux transmis ne seront jamais enregistrés sur les smartphones des utilisateurs et seront censés ne concerner que les « incivilités graves » et « situations critiques » intervenant sur la voie publique ou dans des lieux ouverts au public, conformément aux termes de la charte d'utilisation de l'application.

Si votre rapporteur ne souscrit pas à une telle analyse (encadrement par le seul cadre juridique de la protection des données personnelles) s'agissant de l'instauration pérenne d'un système institutionnel basé sur la captation et l'enregistrement d'images et de sons par l'autorité publique, tant celui-ci toucherait aux questions de vie privée et de libertés publiques, il se demande si la Commission pourrait envisager, s'agissant de la phase d'expérimentation, de ne pas avancer l'argument du défaut de base légale

---

1 En particulier, dans sa décision n°2011-625 relative à la loi d'orientation et de programmation pour la performance de la sécurité intérieure, le Conseil a censuré les dispositions autorisant toute personne morale à mettre en œuvre, pour des finalités de lutte contre les atteintes aux personnes et aux biens (agressions, vols), des dispositifs de surveillance au-delà des abords « immédiats » de ses bâtiments, ainsi que celles permettant aux personnes publiques de confier à des opérateurs privés le soin d'exploiter des systèmes de vidéoprotection sur la voie publique et de visionner les images pour leur compte. Il a en effet jugé que « *chacune des dispositions en cause conduisaient à déléguer une mission de surveillance générale de la voie publique et que, par conséquent, elles méconnaissaient l'exigence, résultant de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789, selon laquelle la garantie des droits est assurée par une «force publique». Ce qui était en cause, dans les dispositions contestées, est le caractère public de ce pouvoir de police administrative générale. Le maire de la commune dispose d'un pouvoir de police administrative générale qu'il n'exerce certes pas en qualité d'agent de l'État mais cela ne permet pas que ce pouvoir soit délégué à des personnes privées* » (extrait de son commentaire sur la décision en question). C'est ainsi que l'article R252-3 du CSI, relatif aux caméras installés aux abords des établissements privés, prévoit que « *la ou les caméras composant le dispositif de vidéoprotection sont déconnectées des caméras installées à l'intérieur du lieu ouvert au public de manière à ce que le responsable ou ses subordonnés ne puissent avoir accès aux images enregistrées par la ou les caméras extérieures* ».

qui remettrait en cause la licéité de cette dernière. En effet, celle-ci aura été limitée dans le temps et dans l'espace et quelque peu contrôlée dans ses conditions de mise en œuvre, en particulier du fait de l'absence d'enregistrement des flux audiovisuels transmis au CSU : la « simple » connexion en temps réel à celui-ci aura présenté un moindre risque de traçage des individus dans l'espace public et pourrait dès lors être appréhendée comme un dispositif de « signalement enrichi » plutôt que comme un dispositif de « vidéo étendue ».

Cependant, l'expérimentation ayant de fait déjà été menée, l'avis de la CNIL n'a d'intérêt qu'au regard d'une éventuelle généralisation de « Reporty » qui emporterait selon la CIL un enregistrement des données. Votre rapporteur estime ainsi qu'il n'y a plus lieu de se prononcer sur les conditions de cette expérimentation mais sur celles envisagées pour sa pérennisation.

En tout état de cause (nécessité ou non d'un encadrement législatif spécifique), votre rapporteur relève que si la collecte de flux visuels et sonores via l'application « Reporty » devait être considérée comme étant mise en œuvre, au moins pour partie, pour le compte de l'Etat, en ayant notamment pour objet de prévenir, constater et poursuivre des infractions pénales[2], ce traitement devrait être autorisé, à l'instar de celui réalisé par les forces de l'ordre via leurs caméras mobiles, par un acte réglementaire pris après avis de la CNIL. A cet égard, le champ très large des incidents justifiant l'utilisation de l'application, ainsi que l'enregistrement des flux à des fins probatoires, semblent plaider en faveur d'une telle analyse. Conformément à l'article 26 de la LIL, cet acte réglementaire devrait avoir la nature d'un décret dès lors que pourraient être concernées des données sensibles au sens de l'article 8 de la loi « Informatique et Libertés » (analyse effectuée par la CNIL lors de son instruction du dossier « caméras mobiles des forces de l'ordre »).

B. L'appréciation du dispositif envisagé au regard des principes de protection des données personnelles

1. Sur la proportionnalité du traitement mis en œuvre

Si la finalité poursuivie – renforcer la réactivité des forces de l'ordre lors de troubles à l'ordre public, « prendre la température » des incidents pour mieux dimensionner les moyens à déployer pour y faire face, voire constater les infractions commises et poursuivre leurs auteurs – peut en elle-même être considérée comme légitime, votre rapporteur considère que **le dispositif envisagé emporte des risques particulièrement importants de surveillance incontrôlée et d'atteintes à la**

[2] En 2006, avant de saisir la CNIL d'un projet d'arrêté autorisant la mise en œuvre de traitements automatisés dans les communes ayant pour objet la recherche et la constatation des infractions pénales par leurs fonctionnaires et agents habilités, le ministère de l'Intérieur lui a indiqué que les traitements en cause devaient nécessairement être considérés comme étant « mis en œuvre pour le compte de l'Etat », dès lors que les agents de police municipale exerçaient leurs missions de police judiciaire (article 21 du Code de procédure pénale) sous le contrôle du procureur de la République, en leur qualité d'agents de police judiciaire adjoints (leurs missions de police administrative, telles que précisées aux articles L.2212-2 à L.2213-31 du code général des collectivités territoriales, relèvent en revanche de la responsabilité du Maire).

vie privée des administrés. De tels risques peuvent être jugés comme revêtant un caractère excessif au regard du but recherché et des autres dispositifs d'ores et déjà mis en place par la collectivité à des fins de sauvegarde de l'ordre public et de signalement des incidents aux services habilités.

En effet, dans son analyse de la proportionnalité du traitement envisagé, votre rapporteur a pu relever les éléments suivants :

- les dispositifs de captation d'images et de sons sont en eux-mêmes de nature particulièrement intrusive en ce qu'ils fournissent de nombreuses informations sur les personnes intéressées, telles que leur présence et leur comportement en un endroit et à un moment donnés, ainsi que la teneur d'éventuelles conversations privées ; ainsi, la CNIL fait preuve d'une grande vigilance quant à la proportionnalité des systèmes de vidéosurveillance et se montre traditionnellement très réservée sur le couplage de ceux-ci à des mécanismes d'enregistrement sonore (jugés par principe comme étant excessifs) ; de même, le CSI encadre strictement le recours à ces dispositifs, qu'ils soient exploités isolément ou cumulativement (ses dispositions sur les systèmes de vidéoprotection ne permettent pas l'enregistrement du son, tandis que celles qui l'autorisent pour les caméras mobiles se fondent sur la nature particulière des circonstances dans lequel cet enregistrement intervient et ne permettent la consultation des données qu'*a posteriori* et dans des cas limités) ;

- nonobstant l'obligation de signature d'une charte d'utilisation avant l'exploitation de l'application, la mise à disposition de celle-ci incitera *de facto* les particuliers à multiplier les captations d'images et de sons tirés de leur environnement, sans que le champ des données captées, et *a fortiori* leur caractère strictement nécessaire à l'objectif poursuivi, puisse en amont être filtré par la collectivité ; sera ainsi collecté et enregistré un volume important de données personnelles sans lien direct avec les incidents (passants/témoins non impliqués dans les évènements visés), ou sans rapport réel avec la commission d'une infraction/d'une « grave incivilité» (erreurs d'appréciation/présomptions d'utilisateurs potentiellement fondées sur des préjugés discriminatoires), ou encore sans objet au regard des missions de la police municipale ou sans respect des termes de la charte (ex. : utilisation de l'outil dans le cadre de règlements de compte personnels ou dans des lieux privés) ;

- la définition par la charte des cas d'utilisation de l'application est en outre suffisamment large (dépôts sauvages d'encombrants et de déchets sur la voie publique) pour permettre par exemple la captation de l'image et de l'environnement sonore d'une personne laissant un objet sur le trottoir le temps d'aller chercher sa voiture pour le récupérer, ou encore d'une personne jetant dans le caniveau un mégot de cigarette ou ne ramassant pas les déjections de son chien sur la voie publique ; or, si l'article R633-6 du Code pénal incrimine expressément de tels comportements, il n'est guère évident que leur niveau de « gravité » soit tel (il ne s'agit pas de faits délictuels mais « juste » contraventionnels) qu'il justifie de potentielles atteintes à la vie privée des

personnes entrant dans le champ de la caméra et du microphone de l'utilisateur de l'application ;

- au regard des risques non négligeables de « dérapages » précédemment exposés, dont la Ville elle-même semble d'ailleurs avoir pleinement conscience puisqu'elle y consacre tout le point III de sa charte d'utilisation (liste des comportements proscrits), il ne paraît pas pouvoir être admis qu'une autorité publique soit *de facto* à l'origine, ou du moins favorise pour disposer de preuves en matière de commission d'infractions, la réalisation par les administrés, de façon consciente ou inconsciente, d'actes potentiellement illicites via le recours à des captations clandestines d'images/sons pouvant porter atteinte à la vie privée de personnes ;

- par ailleurs, la Ville de Nice dispose déjà d'un certain nombre de dispositifs visant à la sécuriser, à mettre un terme aux troubles à l'ordre public et à faire participer ses citoyens à la sauvegarde de celui-ci ; en effet, elle est particulièrement outillée en systèmes de vidéoprotection (près de 2000 caméras, soit presque 2 fois plus que ce qui existe pour l'ensemble de la Ville de Paris) ; les évènements, d'ordre infractionnel ou non et nécessitant une intervention plus ou moins urgente des forces de l'ordre et/ou services de secours, peuvent être signalées par les personnes ayant souhaité intégrer le réseau des « voisins vigilants » et, plus largement, par les administrés au moyen d'un appel de la police municipale, du « 17 » ou du « 112» (saisines des services de police nationale et de secours), ou encore de l'utilisation du dispositif « Allo Mairies » (par exemple, pour le nettoyage d'un tag sur un bien public) ;

- de plus, indépendamment du recours à une telle application, les citoyens pourront toujours transmettre aux forces de l'ordre des enregistrements audiovisuels de situations « inquiétantes » dont ils auront été témoins ou victimes ;

- enfin, il semble qu'un tel dispositif revête un caractère potentiellement contre-productif, sa mise en œuvre étant susceptible de porter atteinte à la sécurité des utilisateurs de l'application, comme à celle des personnes se trouvant réellement dans une situation de danger ; en effet, le président du Syndicat de défense des policiers municipaux a lui-même indiqué : « *nous pensons qu'il n'est jamais bon de déléguer un service public de sécurité à des citoyens. Sur tous les utilisateurs de l'application, quelle va être la part de ceux qui vont découvrir des incivilités de manière inopinée et la part de ceux qui, au contraire, vont se sentir investis d'une mission, traquer le délit ou l'incident et donc s'exposer de façon dangereuse ? Nous estimons que la constatation des infractions doit uniquement relever de la police et que la sécurité doit rester entre les mains de professionnels* » ; de même, ce dispositif pourrait bien fonctionner dans un sens *in fine* défavorable aux personnes victimes d'infractions, dont la situation risque de se retrouver noyée dans tous les flux d'images, sons et appels alors transmis au service de police municipale (pour reprendre l'expression figurant sur le site internet de la préfecture de police de Paris : « *Abuser des numéros d'urgence nuit gravement à ceux qui en ont besoin* »).

Au regard de tout ce qui précède, votre rapporteur exprime de très fortes réserves sur la proportionnalité du dispositif expérimenté, la recherche d'une amélioration de la réactivité et de l'efficacité des forces de l'ordre ne lui paraissant pas légitimer l'institutionnalisation d'un système de contrôle où, suivant une logique de défiance, chacun est incité à surveiller l'autre et à se transformer en justicier, au prix d'une multiplication des risques d'atteinte à la vie privée des citoyens.

2. Sur la loyauté de la collecte

Conformément au cadre juridique de la protection des données personnelles, les traitements de telles données doivent être effectués « *de manière loyale* » (art. 6 de la loi « Informatique et Libertés » et articles 12 du RGPD et de la directive « police-justice » qui posent un principe général de transparence et de facilitation de l'exercice des droits).

Or, **si ce cadre juridique prévoit des dérogations à l'obligation d'information des personnes concernées – en particulier lorsqu'une telle information ferait obstacle à la satisfaction des objectifs poursuivis en matière de prévention, de recherche, de constatation ou de poursuite d'infractions pénales** (art. 32 de la loi, art. 13 de la directive), **la CNIL, dans son avis de 2015 sur le projet de décret autorisant le port de caméras individuelles par les agents de la police et de la gendarmerie nationale, a indiqué qu'« *une telle information, obligatoire en matière de vidéo, constitue une garantie essentielle » en ce qu'elle est « de nature à assurer une meilleure proportionnalité des traitements projetés* », ainsi que l'effectivité du droit d'accès des intéressés**. Le législateur a rejoint cette analyse puisqu'aux termes de l'article L. 241-1 du CSI, outre l'information générale livrée au public via leurs sites institutionnels, les autorités publiques devront veiller à ce que les caméras soient « *portées de façon apparente* » par leurs agents habilités et qu' « *un signal visuel spécifique indique si la caméra enregistre* ». Le déclenchement de l'enregistrement doit de surcroît faire l'objet d'une information des personnes filmées, sauf si les circonstances l'interdisent.

Naturellement, l'utilisation de l'application « Reporty », qui vise à attirer discrètement l'attention des forces de l'ordre, ne saurait répondre à de telles exigences d'information individuelle – seule une information générale sur le site internet de la collectivité ou par voie d'affichage pourrait être réalisée – et emportera ainsi en pratique la collecte d'images et de sons à l'insu des personnes concernées.

Conclusion

Pour conclure, votre rapporteur considère que la Présidente devrait faire part à la Ville de Nice des réserves majeures qu'inspire à la Commission le recours à cette application. Il lui semble également que l'argument tiré du défaut de base légale devrait permettre à notre institution de s'opposer clairement à sa pérennisation dans les conditions envisagées.

En outre, il serait opportun que la collectivité fournisse à la CNIL un bilan d'évaluation de l'expérimentation, de façon à ce qu'elle puisse étayer son analyse et se prononcer en pleine connaissance de cause dans l'hypothèse où ce dispositif aurait vocation à être pérennisé.

Enfin, la CNIL devra nécessairement attirer l'attention du ministère de l'Intérieur sur les différentes problématiques qu'aura soulevée cette expérimentation. Il s'agira en particulier de recueillir ses observations sur le sujet et de l'inviter à intervenir auprès des autorités publiques compétentes, pour que soit clarifiées les conditions de légalité de ce type de dispositif dont on peut craindre qu'il ne reste pas isolé.

Liste des annexes

ANNEXE 1 : charte d'utilisation de l'application mobile pilote REPORTY

VILLE DE NICE
www.nice.fr

Application mobile pilote « Reporty »

Charte d'utilisation

Contexte

Près de 2000 personnes (agents de la Ville de Nice, de la Métropole Nice Côte d'Azur et du CCAS de Nice ; voisins-vigilants officiant sur la commune de Nice ; membres des comités de quartier de la commune de Nice) ont accepté *-sur la base du volontariat-* de tester jusqu'au 10 mars 2018 l'application mobile pilote « Reporty ».

Ci-après dénommés « les utilisateurs » ou « l'utilisateur »

Il s'agit d'un projet d'expérimentation permettant de tester les fonctionnalités de cette application sur le territoire de la Commune.

Le présent document a pour objet de fixer les limites d'usage et les bonnes pratiques à respecter lors de l'utilisation de l'application mobile pilote « Reporty ».

L'accès à cette application ainsi que son utilisation sont soumis à la signature préalable de la présente charte qui vaut acceptation de ses termes et conditions.

En cas de manquement aux dispositions de la présente charte, l'utilisateur en défaut pourra se voir automatiquement désinscrit du service.

I. L'application mobile pilote « Reporty »

Cette application vise à permettre à un utilisateur -à l'aide de son smartphone- de signaler à la Police Municipale de la ville de Nice une incivilité grave ou une situation critique, dont il serait témoin ou victime, en transmettant en temps réel au Centre de Supervision Urbain (CSU) une vidéo (image et son) de son environnement immédiat et des évènements en cours, ou un« tchat » en mode texte quand la qualité réseau n'est pas bonne, ou un appel téléphonique.

Cette application doit s'entendre comme un outil venant en complément de ce qui existe déjà en termes de signalements effectués auprès des services compétents (standard téléphonique de la police municipale ; standard téléphonique du service « Allo-Mairie »). Elle a pour objectif *-dans des cas expressément définis par la présente charte-* de permettre à la police municipale une prise en charge efficiente des évènements.

L'utilisation de ce service est conditionnée par le respect en amont de plusieurs étapes :

- le téléchargement de cette application nécessite l'inscription préalable de l'utilisateur à ce service (nom ; prénom ; numéro de téléphone mobile) ;
- un tutoriel de présentation de cette application est dispensé en présentiel à l'utilisateur une fois l'application téléchargée ;
- la présente charte d'utilisation est soumise à la signature de l'utilisateur une fois le tutoriel de présentation dispensé ;
- un code personnel d'activation de l'application est adressé à l'utilisateur (par SMS) une fois la présente charte d'utilisation signée.

Pour permettre à l'application d'accéder à certaines fonctions du smartphone, l'utilisateur devra autoriser l'accès à la géolocalisation (uniquement quand l'application est active, *c'est-à-dire pendant le temps durant lequel l'utilisateur est connecté en temps réel à la police municipale*), au micro et à la caméra.

Lorsque l'application est lancée *-c'est-à-dire lorsque l'utilisateur utilise ce service*, la connexion s'effectue automatiquement avec le CSU (sous condition d'une couverture réseau minimale).

Les vidéos qui sont transmises ne sont pas enregistrées sur le smartphone de l'utilisateur.

Ces vidéos sont exclusivement enregistrées au CSU.

Lorsque l'utilisateur utilise ce service, son identité ainsi que sa localisation géographique sont automatiquement et exclusivement transmises au CSU.
La connaissance immédiate de la localisation géographique de l'utilisateur permet à la Police Municipale de prendre en charge l'évènement de manière efficiente.

La connaissance immédiate de l'identité de l'utilisateur permet à la Police Municipale d'éviter les abus dans l'utilisation de ce service.

II. Champ d'application de « Reporty »

Afin d'éviter une utilisation détournée de ce service et un engorgement du CSU, le champ d'application de Reporty est strictement défini :

- l'application Reporty ne peut être utilisée que dans des lieux publics et ne doit pas servir à filmer des lieux privés ;
- les faits doivent se dérouler sur le territoire de la Commune de Nice ;
- les faits doivent revêtir un caractère de gravité et d'urgence ;
- les faits doivent être en cours de réalisation (pas de signalement après coup) ;
- Situations critiques visées : actes de violence ; vol ; enlèvement ; attentat ; effondrement ; inondation ; incendie ; accident ;
- Incivilités graves visées : dépôts sauvage d'encombrants ou de déchets sur la voie publique, tags conséquents sur un bien public.

III. Utilisation de l'application mobile pilote « Reporty »

Les utilisateurs participent à cette expérimentation sur la base du volontariat.

Avec cette application, les utilisateurs disposent de la faculté de signaler à la Police Municipale une incivilité grave ou une situation critique en transmettant une vidéo, un tchat ou un appel en temps réel ; il s'agit d'une faculté car les utilisateurs ne sont pas tenus d'utiliser cette application (décision laissée à leur libre appréciation).

La participation à cette expérimentation ne doit pas conduire les utilisateurs à surveiller leur environnement.

Cette application doit être utilisée avec la plus grande vigilance. Les utilisateurs doivent faire preuve de discernement dans la perception des faits dont ils sont les témoins.

Les signalements opérés ne doivent pas avoir pour objet de perturber le bon fonctionnement de la police municipale.

Les signalements abusifs, en particulier par leur nombre, leur caractère répétitif ou systématique, exposeront leur auteur à un retrait de cette application (le caractère abusif d'un signalement s'appréciant au cas par cas).

Cette application ne doit pas être utilisée pour régler une situation tendue, voire un contentieux, avec autrui, c'est-à-dire que cet outil ne doit pas être utilisé comme un moyen pour se venger d'autrui par rapport à une situation personnelle.

L'utilisation de cette application doit s'effectuer dans le cadre des textes législatifs et règlementaires en vigueur. En particulier, elle ne doit pas être utilisée au volant.

L'utilisation de cette application ne doit pas conduire les utilisateurs à se mettre en danger.

L'utilisation de cette application ne doit pas conduire les utilisateurs à se substituer aux forces de l'ordre (les utilisateurs ne doivent pas intervenir eux-mêmes).

Dans tous les cas, les utilisateurs doivent respecter les injonctions que le personnel de la police municipale peut être amené à faire par l'intermédiaire de l'application.

III. Protection des données à caractère personnel

Les données personnelles vous concernant sont collectées et traitées de manière loyale et licite, conformément aux dispositions de la loi n° 78-17 du 06 janvier 1978, modifiée, relative à l'Informatique, aux Fichiers et aux Libertés.

Le traitement de vos données repose sur votre consentement que vous pouvez retirer à tout moment.

Les traitements de données à caractère personnel mis en œuvre poursuivent les finalités suivantes :

- gestion et suivi des utilisateurs de l'application mobile pilote « Reporty » ;
- gestion des signalements opérés ;
- gestion des situations d'abus éventuels ;

Les données d'identification vous concernant ainsi que les jours et heures de vos appels téléphoniques et de vos tchat sont conservées le temps de l'expérimentation.

Les flux transmis par l'application (images ; sons ; géo-localisation ; tchat) sont conservés 10 jours avant d'être automatiquement effacées.

Vos données d'identification sont réservées à l'usage du personnel habilité de la direction des systèmes d'information et de la police municipale

Les flux transmis par l'application sont réservées à l'usage du personnel habilité de la police municipale.

En cas de réquisition judiciaire, ces flux et données d'identification pourront être transmis aux autorités judiciaires.

Vous disposez d'un droit d'accès, de rectification et d'opposition aux données qui vous concernent. Vous disposez également du droit d'organiser le sort de vos données post-mortem. Ces droits peuvent être exercés en vous adressant à la police municipale, 5 Place du Général de Gaulle, 06000 NICE ou au 04 93 53 53 53.

Je soussigné(e) Madame – Monsieur *(rayer la mention inutile)* .....

Déclare avoir pris connaissance des dispositions de la présente charte et m'engage à les respecter.

Fait à ....., **le** .....

Signature