Police municipale et fichiers informatiques

par Mélanie Fèvre
Formatrice au Centre National de la Fonction Publique Territoriale (CNFPT)
Chargée de cours à l'Université de Reims Champagne-Ardenne
Docteur en Droit

Tantôt décriée voire considérée comme illégitime, la police municipale ne laisse, tant soit peu, personne indifférent. C'est pourtant oublier que la police municipale est bien la plus ancienne des polices. Etymologiquement, le mot « poli » signifie cité, il appartient donc à la police de préserver l'ordre public dans cette cité. La police municipale est, en effet, avec la gendarmerie, le plus ancien corps de police. Toutes deux sont issues, historiquement, des guets urbains. Pendant les années 1970, et au début des années 1980, le développement accru de la délinquance, mais également l'opinion publique de plus en plus sensible aux questions de sécurité, vont engendrer une évolution et un développement des polices municipales. La loi du 28 juillet 1978 fait de l'agent de police municipale un agent de police judiciaire adjoint[1], il est reconnu en tant qu'agent de la force publique depuis 1972. Le rapport Bonnemaison de 1982, concernant le développement de la police municipale dans le cadre de la mise en œuvre de la politique locale de sécurité, donne un support juridique aux polices municipales. Dans les années 1980, la loi du 2 mars 1982 relative à la décentralisation dispose que « le maire est chargé sous la surveillance de l'administration supérieure de la police municipale » et la loi du 26 janvier 1984 définit les agents de police municipale comme des fonctionnaires territoriaux. Par la suite, le décret du 24 août 1994, abrogé par le décret du 17 novembre 2006, va encadrer le statut particulier du cadre d'emploi des agents de police municipale. Puis, c'est incontestablement, la loi du 15 avril 1999 relative au statut des agents de police municipale et augmentant les compétences de ceux-ci dans de nombreux domaines, qui marque un tournant important dans l'encadrement et la professionnalisation de la police municipale.

1. Article 21 du Code de procédure pénale.

Professionnalisation qui s'accroît également avec la création, par le décret du 1er août 2003, d'un Code de déontologie des agents de police municipale et qui trouvera son point d'orgue avec le décret du 3 août 2007 encadrant l'armement. Or c'est bien là que réside tout le paradoxe : une volonté politique et juridique de professionnaliser la police municipale, de s'appuyer sur ses 21 000 agents[2] en période d'état d'urgence, tout en ne lui accordant pas pleinement les outils nécessaires à sa mission, comme c'est le cas de l'accès direct à certains fichiers informatiques. Tel est le sens du discours du ministre de l'intérieur de l'époque, Bernard Cazeneuve, qu'il prononce en juin 2015 après les évènements tragiques de janvier 2015, devant la commission nationale consultative des polices municipales. Rappelant qu'il a en mémoire les meurtres des policiers municipaux Clarissa Jean-Philippe, le 8 janvier 2015 à Montrouge, et d'Aurélie Fouquet, assassinée le 20 mai 2010 à Villiers-sur-Marne, il s'engage à un accompagnement étatique fort envers les polices municipales : « Face à la violence, à la délinquance et à la criminalité, les policiers nationaux, les gendarmes et les policiers municipaux sont donc tous en première ligne (…). Si la sécurité de nos concitoyens est avant tout une mission de l'État – et celui-ci assume pleinement ses responsabilités – je sais aussi combien est important le rôle joué par nos polices municipales dans leurs missions de prévention, de présence dissuasive, de médiation ou bien de répression (…). Nous sommes donc engagés dans un processus d'harmonisation des polices municipales qui respecte leur identité propre et leurs spécificités dans notre dispositif global de sécurité (…). Trop longtemps, les gouvernements successifs – de tous bords – ont tergiversé, il faut avoir l'humilité de le reconnaître. Il était grand temps d'avoir enfin le courage de prendre les décisions qui s'imposaient, notamment pour assurer la sécurité des hommes et des femmes qui s'engagent dans la police municipale (…). Nous renforçons la coordination avec les services de police nationale et les unités de gendarmerie, ainsi que le partage d'informations ou encore l'accès aux informations contenues dans certains fichiers qui sont utiles à l'action quotidienne des policiers municipaux ». Il affirme ensuite la nécessité pour les policiers municipaux d'avoir un accès direct aux informations contenues dans certains fichiers nationaux tels que le Fichier des véhicules volés (FVV) ou bien le Système d'immatriculation des véhicules (SIV), ou encore le Système national des permis de conduire (SNPC). En effet, la pratique démontre à quel point l'accès indirect à certains fichiers demeure problématique sur le terrain. « Lorsqu'un policier municipal se trouve face à une voiture qui pose problème, il doit passer par la police nationale qui, seule, a accès à ce fichier. Par ailleurs, lorsqu'il s'agit d'une liste de plusieurs numéros de véhicules en infraction ou dont la présence est suspecte, il est souvent demandé au policier municipal de se déplacer au commissariat, ce qui lui fait perdre un temps considérable, comme à l'agent de police nationale ». Tel est un des arguments issus de la pratique avancé dans la proposition de loi de

2. Chiffre du ministère de l'intérieur pour 2015. Club prévention-sécurité, La Gazette. 11/05/2016.

2016[3] visant à systématiser l'accès direct aux fichiers d'identification des véhicules et des personnes pour les policiers municipaux et prend, dans ce contexte tout son sens. Actuellement, les agents de police municipale, agissant sous le contrôle du maire, responsable du traitement, sont destinataires, au sens de la loi CNIL[4] de certains fichiers, soit de manière directe soit de manière indirecte (**I**), cet accès engageant la responsabilité de ces deux acteurs (**II**).

I. L'accès encadré de la police municipale aux fichiers informatiques

Le maire s'appuie sur sa police municipale dans son rôle de police administrative et de police judiciaire. Dans ce cadre, force est de constater que l'utilisation de fichiers informatiques se révèle évidemment incontournable. Toutefois, elle doit s'appliquer en respectant les règles de la CNIL[5] qui fixe les conditions de leur utilisation tout en déterminant les responsables de traitement et les destinataires (**A**). Or, les policiers municipaux sont loin d'être systématiquement des destinataires directs (**B**).

A. Des fichiers respectant le cadre juridique imposé par la CNIL

La loi du 6 janvier 1978[6] modifiée, loi emblématique s'il en est, prévoit un encadrement juridique de l'utilisation de traitements de données à caractère personnel et expose les grands principes qui doivent guider l'utilisation de fichiers. « L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. ». Par ailleurs, la loi caractérise la donnée personnelle comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. ». Enfin, elle définit le traitement comme « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé

3. Proposition de loi n° 3818 Assemblée Nationale le 8 juin 2016.
4. Loi n° 78-17 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi du 6 août 2004 Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
5. Commission nationale informatique et libertés.
6. Op. cit.

utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. ». Dans le cadre de la police municipale, il y a deux types de fichiers utilisés correspondant bien à la définition du traitement de données à caractère personnel décrit par la CNIL : ceux qui sont utilisés dans le cadre d'infractions et ceux qui sont utilisés hors infraction. Dans les deux cas, le responsable du traitement est soit le ministre de l'intérieur soit l'exécutif de la commune autrement dit le maire, et ce, selon la nature du fichier.

Les obligations d'un responsable de traitement, les personnes habilitées à devenir les destinataires du traitement[7], les types de données pouvant faire l'objet d'une collecte[8], les modalités de récolte et la conservation des données sont prévues pour chaque fichier par la CNIL. « Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ». Le chapitre IV de la loi encadre juridiquement la notion de responsable de traitement et de sous-traitant. Ainsi, l'article 25 précise les obligations pesant sur le responsable de traitement qui doit mettre en œuvre « les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité ».

L'article 6 de la loi pose également les principes de finalité, de proportionnalité et d'exactitude. À titre d'exemple, dans sa délibération n° 2014-19, la CNIL a précisé que les dispositions du code de la sécurité intérieure applicables en matière de lecture automatisée des plaques d'immatriculation « devaient limiter la mise en œuvre de ces dispositifs aux seuls services de police, gendarmerie nationales et douane ». Les communes ne peuvent donc pas les mettre en œuvre. En outre, elle précise « que la collecte massive des numéros de plaques d'immatriculation, sans justification particulière, pourrait conduire à identifier toutes les personnes empruntant la voie publique à l'entrée ou la sortie du territoire d'une commune. Une telle collecte serait dès lors susceptible de méconnaître le principe de proportionnalité ».

Par ailleurs, un traitement ne peut porter sur des données à caractère personnel que s'il est collecté de manière loyale et licite pour des finalités déterminées, explicites et légitimes. Les données ne pouvant pas être traitées ultérieurement

7. Ibid article 3.

8. Ibid articles 8 à 26 : « les origines raciales », ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, ou celles relatives à la santé et à la sexualité sont interdites, étant qualifiées de données sensibles, sauf exception.

de manière incompatible avec ces finalités. Pour chaque traitement de données à caractère personnel, il y a lieu de se référer à l'arrêté ministériel ou au décret en Conseil d'État l'ayant créé pour vérifier si les agents de police municipale figurent dans la liste nominative des destinataires autorisés.

Lors de manquements sérieux au respect de la loi informatique et libertés, la CNIL a le pouvoir de prononcer des sanctions administratives ou financières. Dans ce cas, la CNIL se réunit en formation contentieuse pour prononcer les sanctions prévues à l'article 45 de la loi. Les sanctions pénales prévues aux articles 226-16 à 226-24 du Code pénal peuvent aussi s'appliquer, la CNIL ayant la possibilité de dénoncer au Procureur de la République les infractions à la loi dont elle a connaissance. En effet, un arrêt du Conseil d'État reconnaît à la CNIL la qualité de tribunal dans l'exercice de son pouvoir de sanction, au sens de l'article 6 de la Convention Européenne des Droits de l'Homme[9]. Mais la CNIL ne peut pas prononcer de peines privatives de liberté, faculté appartenant au juge pénal exclusivement. Lorsque des manquements à la loi sont portés à sa connaissance, la formation contentieuse de la CNIL peut prononcer à l'égard du responsable de traitement fautif un avertissement, lequel peut être rendu public. Dans l'hypothèse où le Président de la CNIL a, au préalable, prononcé une mise en demeure, et que le responsable de traitement ne s'y est pas conformé, la formation contentieuse peut prononcer, à l'issue d'une procédure contradictoire une sanction pécuniaire[10] d'un montant maximal de 150,000 €, et, en cas de récidive, jusqu'à 300 000 €. Cette sanction peut être rendue publique dans la presse. Une injonction de cesser le traitement ; un retrait de l'autorisation accordée par la CNIL en application de l'article 25 de la loi peuvent également être ordonnés. En cas d'urgence et d'atteinte aux droits et libertés définis à l'article 1er de la loi, la formation contentieuse peut décider, à l'issue d'une procédure contradictoire de l'interruption de mise en œuvre du traitement. En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander, par référé, à la juridiction compétente, d'ordonner toute mesure de sécurité nécessaire. À compter de la date de notification de la décision de la formation contentieuse, l'organisme mis en cause dispose d'un délai de deux mois pour former un recours devant le Conseil d'État contre la décision de la CNIL.

Depuis la LOPPSI[11], promulguée le 14 mars 2011 à la suite de la décision du Conseil constitutionnel du 10 mars 2011[12], la CNIL a vu ses pouvoirs renforcés avec de nouvelles compétences de contrôle. En effet, un maire peut procéder à l'installation d'un système de vidéo-protection sur la voie publique ou dans un bâtiment public. L'installation des dispositifs de vidéo-protection est soumise à un régime d'autorisation préalable donnée par les services préfectoraux après

9. CE 19 février 2008 n° 311974.
10. Sauf pour les traitements de l'État.
11. Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
12. Décision n° 2011-625 du 10 mars 2011.

avis de la commission départementale. La CNIL dispose donc d'un pouvoir de contrôle de tous les dispositifs de vidéo-protection installés sur le territoire national, y compris ceux installés sur la voie publique, qui relèvent de la loi du 21 janvier 1995[13]. Elle peut, d'une part, mettre en demeure les responsables de ces systèmes, en l'occurrence les maires par exemple, si elle constate des manquements aux obligations qui s'imposent à eux[14] d'autre part, proposer au préfet d'ordonner des mesures de suspension ou de suppression du système contrôlé.

B. L'accès parcimonieux des policiers municipaux aux fichiers

Dans le respect de la loi informatique et libertés, plusieurs textes permettent ainsi aux agents de police municipale d'être destinataires indirects ou directs des informations contenues du fait de leur qualité d'agents de police judiciaire adjoints. La liste des personnes habilitées à consulter les fichiers de police municipale est strictement limitée. De plus, les agents ne sont habilités à consulter les procédures traitées que dans la limite de leur propre habilitation. Peuvent également être destinataires de ces données et informations recueillies, le maire et l'adjoint en charge des questions de sécurité, les magistrats du parquet, l'officier de police judiciaire territorialement compétent, les agents du Trésor public[15] et les fonctionnaires de la préfecture[16.]

Tout d'abord, il s'agit du système national des permis de conduire (SNPC) issu de l'arrêté ministériel du 29 juin 1992. Ce dernier, combiné à l'article L. 225-5, 5° bis, du Code de la route, prévoit que les agents de police judiciaire adjoints peuvent être destinataires des informations relatives à l'existence, la catégorie et la validité du permis de conduire aux seules fins d'identifier les auteurs des infractions au Code de la route ainsi que du fichier national des immatriculations (FNI) issu de l'arrêté ministériel du 20 janvier 1994, qui prévoit la même règle. Ensuite, ils peuvent bénéficier du système d'immatriculation des véhicules (SIV) issu de l'arrêté ministériel du 10 février 2009 ayant pour objet la gestion des pièces administratives du droit de circuler des véhicules ; des traitements dénommés « registre des fourrières et immobilisations » issus de l'arrêté ministériel du 30 mai 2011 qui définit les missions relatives aux véhicules placés en fourrière mais également du système dénommé « contrôle automatisé » issu de l'arrêté ministériel du 13 octobre 2004 concernant les interceptions automatisées d'excès de vitesse. La circulaire du 25 février 2010 du ministère de l'Intérieur relative à la communication aux services de police municipale rappelle explicitement que

13. Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.
14. Information du public, respect de la durée de conservation des enregistrements, limitation des destinataires des images, etc.
15. Pour les données relatives au recouvrement des amendes.
16. 2° de l'article 4, 2° de l'arrêté de 2009.

les policiers municipaux, pour les besoins de l'accomplissement de leurs missions d'informations contenues dans les traitements de données à caractère personnel, ont accès via les forces étatiques aux SNPC, SIV, FNI. Ils ne bénéficient donc pas d'un accès direct à ces fichiers.

Entre 2003 et 2010, la situation concernant l'accès direct des policiers municipaux aux fichiers informatiques, n'a guère évolué.

C'est par un arrêté du 18 août 2011, modifiant l'arrêté du 15 mai 1996 relatif au fichier des véhicules volés, que le ministère de l'Intérieur autorise les policiers municipaux à avoir accès au fichier des véhicules volés. Selon ce texte, « les policiers municipaux sont destinataires des données à caractère personnel et informations enregistrées dans le fichier, dans le cadre de leurs attributions légales et pour les besoins exclusifs des missions qui leur sont confiées, dans la limite du besoin d'en connaître ».

Concernant le fichier des personnes recherchées, le décret du 14 août 2013 modifiant le décret du 28 mai 2010 permet aux policiers municipaux d'être destinataires, à titre exceptionnel, dans le cadre de leurs attributions et à l'initiative des services de la police et de la gendarmerie nationales, de certaines données et informations contenues dans le fichier des personnes recherchées.

La LOPPSI[17] contient de nombreuses dispositions relatives à l'utilisation de nouvelles technologies informatiques dans le domaine de la sécurité et des fichiers de police. Elle modifie, en profondeur le régime juridique relatif à la vidéo-protection[18]. Le maire ne peut pas déléguer à un tiers prestataire privé le visionnage des images issues des systèmes de vidéo-protection. Seuls des agents communaux investis de pouvoirs de police administrative – c'est le cas des agents de police municipale notamment-peuvent être habilités à visionner les images de la voie publique.

Dans la lignée de la loi du 3 juin 2016[19], une nouvelle étape vient d'être franchie avec le décret du 23 décembre 2016[20] relatif aux conditions de l'expérimentation de l'usage de caméras individuelles par les agents de police municipale dans le cadre de leurs interventions et avec le décret relatif à la mise en œuvre de traitements de données à caractère personnel provenant des caméras individuelles des agents de la police nationale et des militaires de la gendarmerie nationale[21]. Ces textes prévoient que les images ne peuvent être consultées qu'à

17. Op. cit.

18. Article L. 251-2 du code de la sécurité intérieure.

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

20. Décret n° 2016-1861 du 23 décembre 2016 relatif aux conditions de l'expérimentation de l'usage de caméras individuelles par les agents de police municipale dans le cadre de leurs interventions.

21. Décret n° 2016-1860 du 23 décembre 2016 relatif à la mise en œuvre de traitements de données à caractère personnel provenant des caméras individuelles des agents de la police nationale et des militaires de la gendarmerie nationale.

l'issue de l'intervention, par les seules personnes habilitées, dans la limite de leurs attributions respectives et pour les besoins exclusifs d'une procédure judiciaire, administrative ou disciplinaire, ou dans le cadre d'une action de formation des agents. La CNIL[22] a regretté que « malgré ses observations formulées dans ces délibérations, le ministère de l'Intérieur ait maintenu un droit d'accès indirect[23] aux enregistrements des dispositifs mis en œuvre par la police et la gendarmerie nationales, ainsi que par la police municipale. Ce même droit d'accès s'exerce pourtant de façon directe pour les dispositifs mis en œuvre par la SNCF et la RATP et, de manière plus générale, pour l'ensemble des dispositifs de vidéo protection ou vidéosurveillance ». L'autorité précise les formalités préalables pour les dispositifs mis en œuvre par les services de police municipale pour lesquels le maire ou, le cas échéant, l'ensemble des maires des communes concernées, doit envoyer un engagement de conformité à la CNIL.

Par ailleurs, l'arrêté du 4 juillet 2013 autorise la mise en œuvre par les collectivités territoriales, les établissements publics de coopération intercommunale, les syndicats mixtes, les établissements publics locaux qui leur sont rattachés ainsi que les groupements d'intérêt public et les sociétés publiques locales dont ils sont membres, de traitements automatisés de données à caractère personnel ayant pour objet la mise à disposition des usagers d'un ou de plusieurs télé-services de l'administration électronique. Les destinataires sont les agents publics et les autorités légalement habilitées à connaître et à traiter les démarches administratives des utilisateurs du télé-service. Ce traitement concerne un certain nombre de formalités liées au service public notamment s'agissant des polices spéciales et de la voirie comme l'autorisation temporaire de débit de boissons ou l'accès aux voies piétonnes par exemple. Les agents de police peuvent, dans le cadre de leurs missions de polices spéciales, avoir accès directement aux informations contenues dans ces fichiers.

En outre, l'arrêté du 17 mars 2014 crée le « Fichier des objets et véhicules signalés » (FOVeS) qui a « pour finalité de faciliter les recherches de la police et de la gendarmerie », et des agents des douanes habilités pour les actes de police judiciaire, pour ce qui concerne leur « surveillance », leur « restitution » ou leur « découverte ». Selon le texte, les policiers municipaux pourront « être destinataires, dans le cadre de leurs attributions légales et dans la limite du besoin d'en connaître, de tout ou partie des mêmes données et informations ». Ils ne sont pas destinataires directs. Le traitement des données sera issu, précise l'arrêté, des procédures judiciaires ouvertes pour vols ou des déclarations de pertes. S'agissant de ce fichier, la délibération CNIL n'a pas formulé d'objection sur ce fichier qui se substitue, comme le TAJ (traitement d'antécédents judiciaires), aux deux fichiers de police et de gendarmerie Stic et Judex et comportant une mention sur les objets volés.

22. Délibération n° 2016-386 du 8 décembre 2016 portant avis sur un projet de décret en Conseil d'État relatif aux conditions de l'expérimentation de l'usage de caméras individuelles par les agents de police municipale dans le cadre de leurs interventions.
23. Effectué par l'intermédiaire d'un magistrat de la CNIL.

La problématique des fichiers impliquant la police municipale réside dans la pluralité des acteurs concernés. Tout d'abord les citoyens, l'usager concerné par un traitement de données à caractère personnel est celui auquel « se rapportent les données qui font l'objet du traitement »[24]. Puis, les responsables du traitement, le maire ou le président de l'établissement de coopération intercommunale autrement dit l'autorité publique qui détermine ses finalités et ses moyens. Enfin, les personnes qui en raison de leurs fonctions sont chargées de traiter les données c'est-à-dire les agents. Or une différence fondamentale réside dans le fait que les exécutifs sont élus tandis que les policiers municipaux sont fonctionnaires. Ils ont pourtant, tous deux, une responsabilité quant à l'utilisation des fichiers.

II. La responsabilité de l'exécutif et de l'agent en matière de fichier

Le maire, responsable de traitement, est garant sur sa commune du respect du cadre juridique imposé par la loi et par la CNIL (**A**) si tel n'est pas le cas, il peut voir sa responsabilité engagée, tout comme l'agent de police municipale, destinataire du traitement (**B**).

A. Le maire et le respect du cadre juridique des fichiers

Le maire, chef du personnel, est responsable de sa police municipale soit dans le cadre d'opérations de police administrative soit dans le cadre d'opérations de police judiciaire. Depuis un certain nombre d'étapes législatives, à travers la loi du 15 avril 1999 relative aux polices municipales, la loi du 15 novembre 2001 relative à la sécurité quotidienne, la loi du 27 février 2002 relative à la démocratie de proximité, la loi du 18 mars 2003 pour la sécurité intérieure ou encore celle du 31 mars 2006 pour l'égalité des chances, les agents de police municipale ont vu leurs missions s'étoffer ainsi que les moyens mis à leur disposition se densifier.

Dans le cadre de la police administrative et ce en vertu de l'article L. 2212-5 du CGCT, « les agents de police municipale, sans préjudice de la compétence générale de la police nationale et de la gendarmerie nationale, exécutent, dans la limite de leurs attributions et sous l'autorité du maire, les tâches que ce dernier leur confie en matière de prévention et de surveillance du bon ordre, de la tranquillité, de la sécurité et de la salubrité publiques ». Les missions des policiers municipaux en matière de surveillance générale de la voie et des lieux publics s'inscrivent dans le cadre d'une police de proximité nécessitant une coordination avec les services de la police et de la gendarmerie nationales dans le cadre de conventions. Ils bénéficient, pour ces missions de prévention, d'un accès à certains fichiers. Dans sa délibération 17 juillet 2008, la CNIL autorise donc, hors des missions liées

24. Article 2 de la loi de 6 août 2004 op. cit.

aux infractions, la création de fichiers de traitement automatisé de l'information dans un poste de police municipale. Ce fichier permet ainsi « la mise en œuvre des registres d'accueil physique et téléphonique du public, la gestion des réclamations, des missions et de la "main courante", production des rapports et des procès-verbaux, production de courriers, gestion des carnets de verbalisation, des avis de contravention et du paiement des amendes, fichier des propriétaires de biens placés à leur demande sous la surveillance de la police municipale, fichier des gérants de commerce entrant dans le champ de compétence de la police municipale, fichier des propriétaires de chiens dangereux, fichier des administrés à contacter en cas de circonstances exceptionnelles, production de statistiques d'activité pour le pilotage du service de police municipale et le compte rendu auprès des autorités communales ». La mise en œuvre de ces traitements est subordonnée à l'envoi préalable à la Commission nationale de l'informatique et des libertés, d'une déclaration faisant référence au présent arrêté et précisant le lieu exact d'implantation du traitement automatisé, les modalités d'exercice du droit d'accès. Il appartient au maire, selon l'article 5 de cette délibération, de prendre « les mesures nécessaires pour préserver la sécurité des données tant à l'occasion de leur recueil que de leur consultation, de leur communication et de leur conservation » et de s'assurer que l'accès par les policiers municipaux sera encadré par des identifiants et des mots de passe régulièrement renouvelés ; accès correspondant d'ailleurs à des attributions spécifiques. Mais au-delà, le traitement bénéficie d'un « dispositif de traçabilité mis en œuvre et tenu à la disposition du maire pour lui permettre d'exercer sa mission de contrôle ».

Dans le cadre de la police judiciaire, et ce, en vertu de l'article 21 du code de procédure pénale, sur le territoire communal, les policiers municipaux ont pour mission « de seconder, dans leurs fonctions, les officiers de police judiciaire ; de rendre compte à leurs chefs hiérarchiques de tous crimes, délits ou contraventions dont ils ont connaissance ; de constater, en se conformant aux ordres desdits chefs, les infractions à la loi pénale et de recueillir tous renseignements en vue de découvrir les auteurs de ces infractions ; de constater, par procès-verbal, les contraventions au code de la route dont la liste est fixée par le décret n° 2000-277 du 24 mars 2000 ; de constater, par rapport, les délits prévus par l'article L. 126-3 du code de la construction et de l'habitation. Ils sont chargés de verbaliser plusieurs catégories d'infractions, notamment les infractions aux arrêtés de police du maire ; au code de l'environnement en ce qui concerne la protection de la faune et de la flore, la pêche, la publicité, à la police de conservation du domaine routier ; à la lutte contre les nuisances sonores ; à la police des gares ; à la législation sur les chiens dangereux ». Les policiers municipaux disposent de plusieurs moyens pour assurer ces missions : le relevé d'identité[25]; le dépistage d'alcoolémie, la rétention du permis de conduire, l'immobilisation et la mise en fourrière de véhicules[26];

25. Article 78-6 du code de procédure pénale.
26. Articles L. 234-3 et L. 234-4 ; L. 224-1 ; articles R. 325-3, L. 325-1 et L. 325-12 ; L. 330-2 et R. 330-3 du code de la route.

l'accès aux parties communes des immeubles à usage d'habitation[27]; les palpations de sécurité dans le cadre des missions confiées par le maire[28]; l'inspection visuelle ou la fouille des sacs et bagages[29]; le carnet de déclarations destiné à recueillir les observations éventuelles des contrevenants verbalisés. À l'occasion de ces différentes missions, l'utilisation de fichiers peut être requise. La police municipale agit sous la responsabilité du maire. Ce dernier, comme l'ensemble des organes exécutifs, est responsable des traitements informatiques mis en œuvre par ses services et de la sécurité des données personnelles qu'ils contiennent. Il peut voir sa responsabilité, notamment pénale, engagée en cas de non respect des dispositions de la loi CNIL. Ainsi, par exemple, ne pas déclarer un fichier qui aurait dû l'être, ne pas prendre toutes les mesures de sécurité pour garantir la confidentialité des informations ou bien encore, utiliser les informations à d'autres fins est susceptible d'être pénalement sanctionné[30]. Comme c'est le cas dans le domaine du secteur privé et de l'entreprise où l'absence de sécurisation de fichiers ou de serveurs est susceptible d'engager la responsabilité. Dès lors qu'il s'agit de stocker, gérer et communiquer par des moyens électroniques, de telles pratiques entrent dans le champ de la définition du traitement automatisé d'informations nominatives et se trouvent donc soumises aux obligations CNIL. Conformément à l'article 26-I de loi Informatique et libertés, ces fichiers sont particulièrement encadrés par la CNIL. Les finalités sont décrites à l'article 5 de l'arrêté, et concernent exclusivement la recherche et la constatation d'infractions au moyen de la tenue du registre de main courante, destiné à enregistrer les interventions des agents verbalisateurs, l'élaboration et le suivi des rapports et procès-verbaux d'infraction, et enfin le suivi du paiement des amendes forfaitaires. Les données ont fait l'objet d'une description précise excluant les fichiers photographiques, ainsi que les informations sur la filiation des victimes, ou sur les personnes mises en cause. Leur durée de conservation est de trois ans maximum, à compter de la date de leur enregistrement. La CNIL considère comme particulièrement important le fait que seuls les fonctionnaires et agents individuellement désignés, par le mécanisme des délégations et spécialement habilités par le maire, soient autorisés à accéder aux données dans la limite de leurs attributions. Aux termes des dispositions de l'article 1 de l'arrêté du 14 avril 2009, les communes qui emploient des agents de police municipale sont autorisées à mettre en œuvre des traitements automatisés de données à caractère personnel relatives aux infractions que ces agents sont

27. Article L. 126-1 du code de la construction et de l'habitation.
28. Article L. 2212-5 du CGCT.
29. Article 96 de la loi du 18 mars 2003.
30. L'article 51 de la loi de 1978 prévoit l'entrave aux actions de la CNIL 15 000 euros et 1 an pour communication de fausses informations relatives aux fichiers ; l'article 226-20 du code pénal : conservation ou traitement des données à caractère personnel au-delà de la durée autorisée 300 000 euros et 5 années ou encore l'article 226-18-1 qui prévoit la mise en œuvre d'un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de celle-ci 300 000 euros et 5 ans.

habilités à constater et à celles dont ils ont connaissance et dont ils rendent compte au maire et au procureur de la République. Cette autorisation s'étend aux gardes champêtres, aux agents de surveillance de la voie publique, aux agents territoriaux spécialement assermentés au Code de la santé publique, aux agents territoriaux assermentés et commissionnés par le maire en matière d'urbanisme, et aux agents territoriaux assermentés en matière de nuisances sonores. Les mesures nécessaires pour préserver la sécurité des données reposent directement et totalement sur le maire. À ce titre, il doit respecter les recommandations de la CNIL. Les traitements relatifs à ces infractions sont subordonnés à l'envoi préalable d'une déclaration faisant expressément référence à l'arrêté du 14 avril 2009 précité. Cette formalité préalable consistera notamment à préciser le lieu exact d'implantation du traitement, les modalités d'exercice du droit d'accès, ainsi que l'engagement spécifique du maire. L'utilisation des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté, est particulièrement encadrée, tant par la loi Informatique et libertés que par la CNIL. Conformément à l'article 26-I de loi, les fichiers d'infractions, de condamnations et de mesures de sûreté doivent être autorisés par arrêtés ministériels, pris après avis motivé et publié de la CNIL. Ils ne peuvent être utilisés que dans les cas strictement prévus par la loi, et par les fonctionnaires spécifiquement visés dans l'arrêté de création. Le recensement des systèmes d'information doit donc se faire en fonction de la structure concernée.

Ensuite, la sécurisation des données[31] est un élément essentiel de la responsabilité des exécutifs que ce soit la sécurisation des accès ou que ce soit la sécurisation des transferts qui peut s'opérer par l'intermédiaire d'un réseau indépendant, par cryptage afin d'assurer la confidentialité des données[32]. L'article 17 de la directive du 24 octobre 1995 complète cette obligation de sécurité qui pèse sur le responsable du traitement. Celui-ci « doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que toute autre forme de traitement illicite. Ces mesures doivent assurer, compte-tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des risques à protéger ».

31. Article 226-17 du Code pénal : la mise en œuvre d'un traitement de données à caractère personnel sans avoir pris les mesures utiles pour préserver la sécurité des données 300 000 euros d'amende et 5 ans d'emprisonnement.

32. Article 29 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés énonce que « toute personne ordonnant ou effectuant un traitement d'informations nominatives, s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées, ou communiquées à des tiers non autorisés ». La violation de cet article 29 est lourdement sanctionnée pénalement par l'article 226-17 du code pénal (cinq ans d'emprisonnement et 300 000 euros d'amende).

À noter que les différents types d'attaques informatiques (virus, vers, chevaux de Troie, bombes logiques) sont également sanctionnés pénalement en droit français par les articles 323-1 à 323-7 du code pénal issus de la loi Godfrain[33]. Aussi, l'arrêté de 2009 prévoit qu'il incombe au maire de prendre les mesures nécessaires pour préserver la sécurité des données tant à l'occasion de leur recueil que de leur consultation, de leur communication et de leur conservation. Il est également prévu la mise en place d'un dispositif de traçabilité permettant de contrôler les conditions d'accès au fichier. En d'autres termes, chaque agent doit être muni d'un code d'accès au fichier qui lui est personnel. À cette fin un administrateur du réseau pourra être nommé. Le fait que les administrateurs des réseaux et des systèmes informatiques aient accès à l'ensemble des informations relatives aux utilisateurs, y compris celles stockées sur leur disque dur, n'est pas contraire aux dispositions de la loi « informatique et libertés ». Ces administrateurs, issus de la filière technique, et non de la filière police municipale[34] sont également tenus au secret professionnel.

B. L'agent de police municipale et l'utilisation illégale des fichiers

Un des risques importants est la divulgation des données. Les agents de la police municipale peuvent être concernés dans la pratique. L'obligation de secret professionnel[35] oblige l'agent public à ne pas divulguer des renseignements ayant un caractère personnel et secret. Cette obligation vise à la protection des usagers du service public. À la différence de la discrétion professionnelle, le secret professionnel protège l'administré et non l'administration. Le manquement au secret professionnel constitue une infraction pénale. Par conséquent, un agent qui de manière intentionnelle divulguerait des informations confidentielles à une personne non autorisée pour les recevoir et ayant pour conséquence de porter atteinte à la considération d'une personne ou à sa vie privée manquerait à cette obligation. L'agent pourrait se voir également infliger, en plus de l'application d'une sanction pénale, une sanction disciplinaire, et ce, même en l'absence de

33. « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 francs d'amende » (article 323-2 Nouveau Code Pénal). De même, « "le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de modifier frauduleusement les données qu'il contient" est puni des mêmes peines (article 323-3 NCP) ».
34. La fonction publique territoriale est composée de huit filières : administrative, technique, animation, sportive, culturelle, médico-sociale, police municipale, sapeur-pompier.
35. Article 226-22 du Code pénal. Communication d'informations à caractère personnel à des personnes non autorisées 300 000 euros et 5 ans d'emprisonnement. L'article 26 de la loi n° 83634 du 13 juillet 1983 et l'article 226-13 du Code pénal : la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

poursuites pénales. L'article 226-22 du Code pénal prévoit des sanctions pénales particulières en cas de violation des dispositions de la loi sur l'informatique, les fichiers et les libertés. En effet, « toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. » La divulgation est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence. Le régime disciplinaire de l'agent est, quant à lui, prévu, pour les policiers municipaux comme pour l'ensemble des agents territoriaux dans l'article 19 de la loi du 13 juillet 1983 portant droits et obligations des fonctionnaires[36] ; l'obligation de probité ayant été renforcée par la loi du 20 avril 2016[37]. S'ajoute à cela l'engagement moral et solennel du serment prononcé par le policier municipal devant le juge du tribunal d'instance. L'assermentation prévue à l'article R. 130-9 du code de la route : « Je jure de bien et fidèlement remplir mes fonctions et de ne rien révéler ou utiliser de ce qui aura été porté à ma connaissance à l'occasion de leur exercice » est destinée à faire prendre conscience à l'agent de l'importance de ses fonctions et de l'obligation de les accomplir scrupuleusement. L'agrément[38] vérifie la moralité et l'honorabilité de l'agent, tandis que la prestation de serment est un engagement de respecter les règles déontologiques comme tout agent ayant des fonctions de police judiciaire.

Les agents de police municipale peuvent également, comme les exécutifs, voir leur responsabilité engagée pour le détournement des données[39]. Prenons l'exemple des véhicules volés. L'arrêté du 18 août 2011 autorise les polices municipales à accéder, par filtre, au fichier des véhicules volés (FVV) géré par les ministères de l'Intérieur et de la Défense. Il permet aux policiers municipaux de participer au signalement des véhicules volés, voire de procéder à l'interpellation

36. Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, articles 89 S de la loi n° 84-53 du 26 janvier 1984 portant dispositions relatives à la fonction publique territoriale, décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires, de décret n° 88-145 du 15 février 1988 pris pour l'application de l'article 136 de la loi du 26 janvier 1984.

37. Loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires.

38. Article L. 412-49 du Code des communes.

39. Article 226-21 « Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

des voleurs. Les agents de police municipale sont amenés à contrôler un grand nombre de véhicules quotidiennement puisque, aux termes de l'article L. 2212-2 du code général des collectivités territoriales, « ils sont compétents pour "tout ce qui intéresse la sûreté et la commodité du passage dans les rues, quais, places et voies publiques" ». Le fichier des véhicules volés relève du ministère de l'Intérieur (direction générale de la police nationale et direction générale de la gendarmerie nationale), il est destiné à faciliter les recherches pour la découverte et la restitution des véhicules volés, la surveillance des véhicules signalés et la recherche et la surveillance des personnes susceptibles d'utiliser un véhicule volé ou signalé. Il comporte les informations nominatives suivantes : l'état-civil (nom, prénom(s), adresse, numéro de téléphone) du plaignant ou propriétaire ; le code de la compagnie d'assurance et le numéro de police ; l'état-civil de la personne recherchée utilisant le véhicule, le motif de la recherche et, le cas échéant, les éléments de signalement ; les caractéristiques permettant l'identification du véhicule (numéro d'immatriculation, numéro de série, de moteur ou de cadre, dénomination, marque, type, genre, couleur, signes distinctifs) ; la conduite à tenir en cas de découverte d'un véhicule volé ou détourné ou en présence d'un véhicule placé sous surveillance. Ces informations servent à la découverte et la restitution des véhicules volés ; la surveillance des véhicules et objets signalés dans le cadre de missions répressives ou préventives ; la découverte et la restitution des objets perdus ou volés. Ces informations à finalité personnelles ou professionnelles ne peuvent être détournées à d'autres fins sous peine de poursuites pénales. La Cour de cassation[40] a confirmé la condamnation à un an d'emprisonnement avec sursis et cinq ans d'interdiction d'exercice des fonctions de la police nationale, d'un policier ayant utilisé le fichier national des automobiles à des fins personnelles, faits relevant de la corruption passive ainsi que de faux et usage de faux pour une utilisation d'un fichier STIC pour faciliter l'immatriculation d'un véhicule. La solution serait, à n'en pas douter, identique, s'agissant d'un policier municipal.

En outre, la collecte illicite de données à caractère personnel par un moyen frauduleux, déloyal ou illicite[41] déclenche la responsabilité de son auteur. Les conséquences de ce type d'infraction sont susceptibles, quand il est condamné pénalement, d'affecter la carrière de l'agent de police municipale. Ainsi, le Conseil d'État[42] a validé la radiation des cadres par le maire d'un agent[43] ayant été condamné par le Tribunal de Grande Instance pour infraction à la loi du 6 janvier 1978 pour avoir participé dans l'exercice de ses fonctions à la mise en œuvre, à l'utilisation et à la dissimulation d'un fichier informatique créé en méconnaissance de ladite loi et contenant des informations nominatives portant atteinte à la vie

40. Cour de cassation, Chambre criminelle, audience publique du 01 avril 2008 N° de pourvoi : 07-84726.
41. Article 226-18 Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite 300 000 euros 5 ans.
42. C.E., 10 juillet 1995 : commune de la Tremblade, garde des Sceaux, n° 148-139.
43. Dr. adm. 1995, n° 626.

privée des habitants de la commune. Le Procureur de la République a considéré que les faits reprochés justifiaient le retrait de l'agrément, nécessaire aux fonctions de policier municipal. En effet, si les agents de police municipale sont nommés par le maire[44], ceux-ci doivent être agréés par le Procureur de la République[45]. Il appartient donc au Procureur d'apprécier si « les faits dont il est avisé sont de nature pour l'agent concerné à compromettre les garanties d'honorabilité requises pour occuper l'emploi de l'administration municipale auquel il a été nommé par le maire[46] » et si la « suspension envisagée de son agrément nécessite d'être mise en œuvre sans délai »[47]. En tout état de cause, ne s'agissant pas d'une compétence liée, le Procureur peut s'abstenir d'un retrait d'agrément même en cas de condamnation pénale, tandis que le maire, lui, est tenu, en cas de retrait de l'agrément, de radier des cadres l'agent de police municipale concerné[48].

Il y a faute disciplinaire chaque fois que le comportement d'un fonctionnaire entrave le bon fonctionnement du service ou porte atteinte à la considération du service dans le public. Il peut s'agir d'une faute purement professionnelle ou d'un comportement incompatible avec l'exercice des fonctions ou portant atteinte à la dignité de la fonction. Or, l'agent a l'obligation d'accéder aux fichiers dans le respect de la loi. Il s'expose aux sanctions disciplinaires classiques prévues dans le statut de la fonction publique, de la moins importante des sanctions, l'avertissement à la plus grave, la révocation. La responsabilité disciplinaire d'un policier municipal peut être engagée en cas de création d'un fichier illicite. Le juge administratif a ainsi confirmé la révocation et le retrait de l'agrément à un policier municipal pour avoir constitué un fichier informatique nominal des administrés de la commune illicitement[49]. De surcroît, la désobéissance hiérarchique prévue par l'article 28 de la loi du 13 juillet 1983 impose à tout fonctionnaire, quel que soit son rang dans la hiérarchie, d'être responsable de l'exécution des tâches qui lui sont confiées. Il doit se conformer aux instructions de son supérieur hiérarchique, sauf dans le cas où l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public et n'est dégagé d'aucune des responsabilités qui lui incombent par la responsabilité propre de ses subordonnés. C'est pourquoi, en matière de fichiers également, la responsabilité des agents peut être engagée pour désobéissance. La juridiction administrative a confirmé la sanction disciplinaire de Melle A, agent de police municipale ayant refusé de procéder,

44. Article L. 412-49 du code général des collectivités territoriales.
45. Et par le préfet.
46. Conseil d'État, section de l'intérieur, avis du 29 septembre 1987 n° 342821.
47. Circulaire du 15 juillet 2013 présentant diverses dispositions relatives à la police judiciaire NOR : JUSD1318536C.
48. C.E., 6 avril 1992, Procureur de la République près le Tribunal de grande instance d'Aix-en-Provence c/ Pirazzelli, Rec., p. 150 ; 10 juillet 1995, commune d'Hyères-les-Palmiers, D.A., n° 625.
49. Cour administrative d'appel de Marseille 2e chambre 30 septembre 2003 inédit au recueil Lebon 30 septembre 2003 affaire n° 99MA01627.

en méconnaissance des ordres donnés, à la destruction d'un fichier de données personnelles relatives aux étrangers résidant sur le territoire communal[50].

À l'heure où la menace terroriste est extrêmement importante et où les policiers nationaux ou municipaux, la gendarmerie, les militaires sont des cibles potentielles, il apparaît essentiel de ne pas leur compliquer la tâche sur le terrain en conditionnant la consultation de certains fichiers à un filtre… Il semble paradoxal, en effet, d'étendre les attributions, les moyens, notamment en terme d'armement de la police municipale et de limiter encore l'accès à certains fichiers. Donner la possibilité d'un accès direct aux fichiers SIV, FVV, FNPC, c'est permettre aux policiers municipaux d'être encore plus réactifs sur le terrain en ne perdant pas de temps dans des procédures superflues, car « ces fichiers sont pour eux un outil de travail essentiel »[51].

Certains crieront sans doute aux risques d'excès voire d'atteintes aux libertés individuelles mais c'est oublier, comme il a été possible de le voir précédemment, que comme les policiers nationaux, les policiers municipaux sont soumis à une déontologie et à un régime disciplinaire strict auquel s'ajoute le risque pénal dans le cas d'une utilisation illégale des données personnelles issues de fichiers. La proposition de loi de 2016 propose donc de compléter ainsi l'article L. 511-7 du code de la sécurité intérieure « les agents de police municipale sont autorisés à accéder directement aux fichiers de traitement des données suivants le système d'immatriculation des véhicules ; le fichier national des permis de conduire ; le fichier des véhicules volés »[52]. Cela permettrait de mettre fin à une situation ubuesque qui freine la police municipale pour l'accomplissement de ses missions alors que certains acteurs privés comme les assureurs ou encore les exploitants d'autoroute ont, eux, accès directement au SIV. Il ne s'agit pas de dénaturer les fonctions de la police municipale ou de conférer aux policiers municipaux des pouvoirs d'enquête qui sont réservés à la police nationale, les fichiers d'antécédents judiciaires et les fichiers de renseignement[53] en étant exclus, mais bien de donner des outils supplémentaires à la police municipale. En tout état de cause, il semblerait que les autorités étatiques aient pris pleinement conscience de l'enjeu, Bruno Le Roux, ministre de l'Intérieur à l'époque, ayant annoncé, que l'accès direct aux fichiers SIV et SNPC, rendu possible par la loi du 22 mars 2016, dite loi Savary[54], « faisait l'objet d'un décret en cours de rédaction »[55].

---

50. CAA Lyon 3e chambre 28 septembre 2010 09LY00531 inédit au recueil Lebon.
51. Exposé des motifs, proposition de loi n° 3818 8 juin 2016.
52. Ibid.
53. Ibid « notamment le système de traitement des infractions constatées – STIC – et le système judiciaire de documentation et d'exploitation – JUDEX ».
54. Loi n° 2016-339 du 22 mars 2016 relative à la prévention et à la lutte contre les incivilités, contre les atteintes à la sécurité publique et contre les actes terroristes dans les transports collectifs de voyageurs.
55. Discours lors de la signature des conventions de coordination entre les polices municipales et les forces de l'ordre à Nancy du 20 janvier 2017. Site du ministère de l'Intérieur.