# Commission nationale de l'informatique et des libertés

## Délibération n° 2013-054 du 7 mars 2013 portant avis sur un projet d'arrêté autorisant la mise en œuvre par les collectivités locales, les établissements publics de coopération intercommunale, les syndicats mixtes et 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 téléservices de l'administration électronique

NOR : *CNIX1317817X*

La Commission nationale de l'informatique et des libertés,

Saisie par le secrétariat général pour la modernisation de l'action publique (SGMAP) d'une demande d'avis sur un projet d'arrêté autorisant 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 téléservices de l'administration électronique ;

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, notamment son article 27-II (4°) et 27-III ;

Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec l'administration, notamment son article 16-A ;

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment ses articles 9 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance citée relatif à la sécurité des informations échangées par voie électronique ;

Vu la délibération n° 2011-107 du 28 avril 2011 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transport publics (autorisation unique n° 15) ;

Après avoir entendu le rapport de M. Gaëtan GORCE, commissaire, et les observations de M. Jean-Alexandre SILVY, commissaire du Gouvernement,

Emet l'avis suivant :

Les ministères en charge de l'intérieur et de la réforme de l'Etat, par l'intermédiaire du secrétariat général pour la modernisation de l'action publique (SGMAP), ont saisi la Commission nationale de l'informatique et des libertés d'une demande d'avis sur un projet d'arrêté autorisant la mise en œuvre par « les entités publiques locales » – à savoir les collectivités territoriales, les établissements publics de coopération intercommunale (EPCI), les syndicats mixtes et les établissements publics locaux qui leur sont rattachés, les groupements d'intérêt public (GIP) et les sociétés publiques locales (PLS) 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 téléservices de l'administration électronique.

Cet arrêté a pour but de prévoir les conditions dans lesquelles un ensemble de services publics accessibles par voie électronique, les « téléservices publics locaux », peuvent être mis à disposition des administrés. Il s'agit principalement de rappeler les règles de sécurité et de protection des données personnelles à mettre en œuvre dans la gestion des échanges dématérialisés entre les administrés et les autorités administratives.

Sans préjudice de l'exercice par les collectivités territoriales de leur droit de créer, après un avis spécifique de la commission, des téléservices en dehors du cadre du présent projet d'arrêté ministériel, ce projet d'arrêté ministériel a vocation à constituer un acte réglementaire unique au sens de l'article 27-III de la loi « informatique et libertés » permettant aux entités publiques locales d'accomplir leurs formalités préalables de manière simplifiée, par le biais de l'envoi à la commission d'un engagement de conformité au cadre ainsi prévu.

A titre liminaire, la commission souligne qu'elle a été largement associée à l'élaboration de ce projet d'arrêté par les administrations compétentes, de même que les associations représentatives des élus locaux. Elle se

félicite de cette démarche de concertation, de nature à permettre la bonne application par les entités publiques locales des principes de protection des données personnelles dans le cadre de la dématérialisation des démarches administratives locales.

*Sur les finalités des traitements :*

Les traitements de données concernés par le projet d'arrêté ont pour finalités de permettre aux administrés d'accomplir en ligne leurs démarches administratives auprès des entités publiques locales et aux agents de celles-ci d'en assurer le traitement et le suivi. La commission considère que ces traitements sont de nature à simplifier les démarches administratives réalisées au niveau des collectivités territoriales et à améliorer les relations entre les administrés et l'administration, A ce titre, elle estime que ces finalités sont déterminées, explicites et légitimes, conformément aux dispositions de l'article 6 (2°) de la loi du 8 janvier 1978 modifiée.

Elle rappelle néanmoins qu'il est nécessaire de limiter la mise en œuvre de traitements de données à caractère personnel à ceux qui sont strictement nécessaires et, en particulier, de ne pas systématiser l'identification d'un administré dès lors qu'une information générale peut être mise à disposition de tout internaute.

Les services susceptibles d'être proposés dans un « bouquet de téléservices » sont groupés en sept secteurs identifiant des catégories d'activités de services publics. L'article 1er du projet d'arrêté précise qu'il s'agit de gérer toutes les démarches administratives s'inscrivant dans les secteurs publics suivants : la fiscalité locale ; le travail et le social ; la santé ; les transports ; l'état civil et la citoyenneté ; les relations avec les élus ; la « vie quotidienne » (comprenant les prestations scolaires et périscolaires, les activités sportives et socioculturelles, l'économie et l'urbanisme, les polices spéciales et la voirie ainsi que les relations avec les usagers).

Cet article établit une liste non exhaustive d'exemples de services publics compris dans chacun de ces secteurs et précise, en outre, que tous les téléservices s'inscrivant dans le même secteur et recueillant les mêmes catégories de données sont inclus dans le périmètre du projet d'arrêté. La mise en œuvre de ces autres téléservices sera ainsi entourée des mêmes garanties que pour ceux qui y sont expressément mentionnés, sans nécessiter de modification de l'acte réglementaire unique.

La commission rappelle que le développement de l'administration électronique ne doit en aucun cas conduire à la création d'un identifiant unique des administrés, au plan local comme au plan national, Elle rappelle également que les traitements de données mis en œuvre dans ce cadre ne doivent pas être utilisés à d'autres fins que l'accomplissement de certaines démarches administratives, et tout particulièrement aux fins d'alimenter d'autres fichiers ou de constituer un fichier de population.

Elle prend dès lors acte que, à sa demande, le projet d'arrêté prévoit en son article 2 que les portails d'accès ou les bouquets de téléservices garantissent l'étanchéité des données entre les différents secteurs de services publics et que la création d'un fichier de population et d'un identifiant administratif unique est interdite.

Néanmoins, la commission estime que cette étanchéité doit également être garantie entre les différents secteurs composant la catégorie « vie quotidienne ». En effet, les services compris dans cette catégorie relèvent d'intérêts publics différents et peuvent nécessiter la collecte des données particulières relevant de la vie privée des administrés, alors même que l'interconnexion de traitements de gestion de services publics relevant d'intérêts publics différents n'est pas autorisée par le projet d'arrêté. Dès lors, la commission estime qu'il n'y a pas lieu de créer un identifiant sectoriel commun à ces activités et qu'il conviendrait de distinguer, comme cela était initialement envisagé, dix catégories de services publics.

A cet égard, elle prend acte de la décision des ministères compétents de suivre la recommandation de la commission.

Ces garanties nécessaires à la protection des données personnelles des usagers de l'administration ne doivent pas pour autant conduire à complexifier l'utilisation des téléservices locaux, et notamment à leur redemander des informations qu'ils auraient déjà fournies à la même entité publique. A cet égard, l'article 2 du projet d'arrêté prévoit qu'au cas où un service traitant a besoin d'une information déjà produite par l'administré auprès d'un autre service traitant il est possible d'obtenir cette information auprès de ce dernier *« après avoir recueilli le consentement exprès et non équivoque de l'usager ».*

Dans la mesure où les données personnelles de l'administré restent ainsi sous son contrôle et où cette disposition permet la bonne application de la loi du 12 avril 2000 qui vise à faciliter les relations entre les citoyens et les administrations, la commission prend acte de cette possibilité.

*Sur les données à caractère personnel collectées :*

L'article 3 du projet d'arrêté précise les catégories de données à caractère personnel enregistrées dans les traitements, en distinguant celles nécessaires pour la gestion de l'accès au portail et celles relatives à l'accomplissement des démarches administratives.

Les téléservices inclus dans le périmètre de l'acte réglementaire unique seront en effet accessibles, au choix de l'administré, par plusieurs procédés d'identification : un couple identifiant/mot de passe, un numéro de téléphone portable, un certificat électronique, une « carte de vie quotidienne » ou encore des clés de fédération, ou « alias », générés par le système et permettant à l'administré d'établir des liens avec ses différents comptes.

Suivant l'architecture du dispositif, déterminée par chaque responsable de traitement, l'administré peut ainsi choisir parmi ces modalités pour accéder aux fonctionnalités proposées par un portail de téléservices.

La fédération d'identités permet à l'administré d'utiliser des services différents sans avoir à s'identifier à nouveau auprès de chacun d'eux au moyen de clés de fédération propres aux différents services. Ainsi que l'a

déjà rappelé la commission, ce dispositif permet ainsi de simplifier l'utilisation de portails de téléservices tout en prévenant la création d'un identifiant administratif unique des administrés et les risques d'interconnexions de fichiers dont les finalités correspondent à des intérêts publics différents.

Concernant les données nécessaires à l'accomplissement de chaque démarche administrative offerte par un téléservice, il s'agit des données qui, figurant sur les formulaires CERFA dématérialisés, sont enregistrées et traitées dans les applications métier des entités publiques locales.

Compte tenu, d'une part, du nombre important des démarches administratives concernées par le projet d'arrêté et, d'autre part, de la variété des données demandées à l'administré, il apparaît impossible de mentionner dans le texte l'ensemble des données susceptibles d'être enregistrées dans ces traitements.

La commission appelle néanmoins à la vigilance de tout acteur public pour ne traiter que les données strictement nécessaires pour rendre le service public dont il la charge, conformément aux dispositions de l'article 6 (3°) de la loi du 6 janvier 1978 modifiée. Elle prend donc que, à sa demande, l'article 3 du projet d'arrêté sera complété sur ce point afin de préciser qu'il s'agit des données *« strictement nécessaires à l'accomplissement des démarches administratives mentionnées à l'article 1er »*.

L'article 3 du projet d'arrêté autorise enfin le traitement de données sensibles au sens de l'article 8 de la loi « informatique et libertés » lorsque ce traitement est *« rendu nécessaire par un texte législatif ou réglementaire »* relatif à la démarche administrative concernée ou lorsque le consentement exprès de l'administré est recueilli. La commission prend acte que la confidentialité de ces données doit, en tout état de cause, être renforcée par des mesures de sécurité supplémentaires.

Elle rappelle néanmoins que la collecte de ces données doit être réalisée directement auprès des personnes concernées et être limitée aux seuls cas strictement nécessaires. Par exemple, la collecte d'informations relatives à la santé des personnes aux fins de mises en place de mesures de secours adaptées ne doit pas se traduire systématiquement par le traitement de données relatives aux pathologies, la saisie des modalités de secours spécifiques que celles-ci imposent pouvant suffire. Il en est de même en matière d'informations relatives au régime alimentaire dans le cadre scolaire, où la mention de la religion des personnes concernées n'apparaît pas nécessaire.

La commission estime, en outre, que les mesures de sécurité complémentaires devraient être également rendues obligatoires pour le traitement des autres données bénéficiant de protections particulières aux termes de la loi du 6 janvier 1978 modifiée, telles que, par exemple, les données relatives aux infractions ou condamnations (article 9) ou le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR). Elle prend acte de ce que l'article 3 du projet d'arrêté sera complété en ce sens.

*Sur la durée de conservation des données :*

Les durées de conservation des données nécessaires à l'accomplissement des démarches administratives varient en fonction du dispositif de l'entité publique locale. Les téléservices offerts par les collectivités peuvent en effet prendre deux formes distinctes.

Si la plate-forme offrant un « bouquet de téléservices » aux usagers ne sert que de « relai » vers des traitements de gestion de l'entité publique locale, la durée de conservation sur la plate-forme est limitée à trois mois et les données sont ensuite détruites.

En revanche, si la plate-forme sert également de plate-forme d'hébergement pour chaque commune (mutualisation des ressources informatiques entre plusieurs entités territoriales), la durée de conservation des données est corrélative à la finalité propre de chaque téléservice.

Sans préjudice des données dont la conservation et l'archivage sont nécessaires au traitement « métier », la commission rappelle que les données collectées pour un téléservice donné ne peuvent être conservées au-delà du délai d'utilité administrative.

*Sur les destinataires des données :*

L'article 5 du projet d'arrêté prévoit que sont destinataires des données les seules autorités légalement habilitées à connaître et à traiter les démarches administratives des utilisateurs du téléservice.

Compte tenu de la diversité des situations des entités publiques locales concernées par ce projet d'acte réglementaire, la commission prend acte de la rédaction générale de cet article. Elle recommande néanmoins que, dans la mesure du possible, les agents des autorités traitant ces démarches administratives fassent l'objet d'une habilitation spéciale et d'une désignation individuelle par leur responsable hiérarchique. De même, elle rappelle que la traçabilité des actions effectuées par ces agents (consultation, modification ou suppression des données) doit être assurée afin de se conformer aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée.

*Sur les droits des personnes concernées :*

Le dernier alinéa de l'article 3 du projet d'arrêté prévoit que la liste des données à caractère personnel enregistrées dans chaque traitement est accessible depuis les téléservices des entités publiques locales. Cette mesure procède de l'obligation d'information incombant aux responsables de traitement, notamment sur le caractère facultatif ou obligatoire des données collectées pour rendre le service et contribue à l'exercice du droit d'accès de l'administré à ses données traitées pour chaque téléservice.

La commission rappelle néanmoins que tout responsable de traitement de l'obligation d'informer les personnes concernées du traitement de leurs données personnelles et de ses modalités principales dans les

conditions prévues par les dispositions de l'article 32 de la foi du 6 janvier 1978 modifiée. Elle prend donc acte que, à sa demande, le dernier alinéa de l'article 3 du projet d'arrêté sera complété sur ce point et rappelle que ces mentions d'information doivent être facilement accessibles pour l'administré et rédigées en des termes clairs et pédagogiques.

Si la commission est favorable au développement de l'administration électronique, elle rappelle que ces outils ne doivent pas être exclusifs d'autres canaux d'accès aux services publics. Elle prend donc acte que l'article 8 du projet d'arrêté prévoit expressément le maintien d'une procédure alternative au téléservice et que cette procédure doit alors permettre l'accès, dans des conditions analogues, à la même prestation de service public.

Enfin, le même article prévoit que les droits d'accès, de rectification et de suppression prévus par les articles 39 et 40 de la loi du 6 janvier 1978 modifiée s'exercent directement auprès du responsable du téléservice. La commission estime que, dans le cadre de tout téléservice, les droits « informatique et libertés » doivent pouvoir s'exercer par voie électronique, ce qui requiert une vigilance particulière sur les mesures de sécurité à mettre en œuvre.

*Sur la sécurité et la confidentialité des données :*

A titre général, la commission souligne qu'au vu de la diversité des téléservices publics locaux et des structures qui les mettent en œuvre, il n'apparaît pas opportun d'imposer dans l'acte réglementaire unique la mise en œuvre de mesures précises garantissant la sécurité et la confidentialité des données. Il semble en effet préférable de prévoir dans le projet d'arrêté le respect de certains principes quant à la sécurité des traitements mis en œuvre, en laissant aux responsables de traitement le soin de déterminer les mesures précises à mettre en œuvre.

La commission prend donc acte que, à sa demande, l'article 6 du projet d'arrêté rappelle expressément les obligations incombant aux responsables de traitement en matière de sécurité et de confidentialité des données traitées. Les obligations concernant la sécurité de tout téléservice de l'administration électronique, notamment l'obligation de sa mise en conformité au référentiel général de sécurité (RGS), ainsi que les dispositions de l'article 34 de la loi « informatique et libertés » sont ainsi rappelées. En particulier, l'article 6 du projet d'arrêté prévoit l'obligation de procéder à la réalisation préalable d'une *« analyse de risques tenant compte du respect de la vie privée »* des administrés.

La commission rappelle que cette étude devra donc considérer, d'une part, les risques d'atteinte à la sécurité des systèmes d'information et leurs impacts sur l'entité publique locale, d'autre part, les risques d'atteinte aux données à caractère personnel et leurs impacts sur la vie privée des administrés. Chaque portail de téléservices locaux étant spécifique, cette étude permettra ainsi de déterminer les mesures adéquates pour traiter ces risques de manière proportionnée, y compris les risques inhérents à la fédération d'identités appliquée mise en œuvre au sein d'une même entité publique locale.

La commission estime ces mesures de sécurité suffisantes. Elle rappelle que cette étude de risques devra être communiquée sur demande à la CNIL. Les mesures de sécurité mises en œuvre et leur amélioration continue doivent être vérifiables, l'ensemble de ces documents devant être tenu à disposition lors de contrôle.

Enfin, dans l'hypothèse du recours à une « carte de vie quotidienne » (CVQ), support unique permettant d'accéder à plusieurs services publics, la commission rappelle que des mesures de sécurité complémentaires doivent être mises en œuvre.

Cette exigence est d'autant plus impérieuse dans l'hypothèse d'une carte multiservices utilisée par plusieurs entités locales pour mutualiser un même service public, au premier rang desquels le transport. En effet, la délibération n° 2011-107 du 28 avril 2011 relative à la gestion des applications billettiques dans le cadre de l'organisation de transports publics (autorisation unique n° 15) dispose que des mesures techniques et organisationnelles doivent être mises en œuvre afin de garantir l'absence de traçabilité des activités et déplacements de l'administré et se prémunir contre les risques d'intrusion et de détournement de données sur les systèmes informatiques. Ces mesures doivent en particulier garantir la stricte étanchéité entre les données des différents services et les identifiants tant techniques que fonctionnels utilisés pour le transport ne doivent pas être utilisés pour d'autres services.

*La présidente,*
I. Falque-Pierrotin