CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Délibération n° 2018-283 du 21 juin 2018 portant avis sur un projet d'arrêté relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé Système d'alerte et d'information des populations « SAIP ».

(demande d'avis n° 2166367)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre de l'intérieur d'une demande d'avis concernant un projet d'arrêté portant création d'un traitement de données à caractère personnel relatif au système d'alerte et d'information des populations (SAIP) ;

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

Vu la directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ;

Vu le code de la sécurité intérieure, notamment ses articles L. 112-1 et L. 112-2 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

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 ;

Sur la proposition de M. Jean-François CARREZ, commissaire, et après avoir entendu les observations de Mme Nacima BELKACEM, commissaire du Gouvernement,

Émet l'avis suivant :

La Commission a été saisie par le ministre de l'intérieur d'une demande d'avis concernant un projet d'arrêté portant création d'un traitement automatisé de données à caractère personnel relatif au système d'alerte et d'information des populations (« SAIP »).

Ce traitement doit permettre aux autorités investies d'un pouvoir de police administrative, telles que le préfet de département ou le maire, de déclencher des moyens d'alerte aux fins de garantir la sécurité civile au niveau national.

Elle relève que le projet qui lui est soumis pour avis relevait, à la date de la saisine, des dispositions de l'article 26-I-1° de la loi du 6 janvier 1978 modifiée qui prévoit qu'un arrêté, pris après avis motivé et publié de la Commission, autorise les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et qui intéressent la sécurité publique. Compte-tenu de l'évolution du cadre juridique relatif à la protection des données à caractère personnel résultant notamment de la prise en

compte des dispositions de la directive (UE) 2016/680 du 27 avril 2016 susvisée, la Commission considère que le traitement projeté doit faire l'objet d'un examen au regard de ces nouvelles dispositions.

Sur la finalité du traitement :

L'article 1er du projet d'arrêté prévoit que le traitement, mis en œuvre par la Direction générale de la sécurité civile et de la gestion des crises, doit « *permettre la diffusion des mesures d'alerte et d'information à destination de la population, à la demande d'une autorité de police administrative, en cas d'événements graves, imminents ou en cours de réalisation, susceptibles de porter atteinte à l'intégrité physique des personnes* ».

La Commission relève tout d'abord que le traitement projeté doit permettre aux autorités investies d'un pouvoir de police administrative d'alerter la population en cas d'événements graves tels que des catastrophes naturelles ou industrielles ou de menaces pour la sécurité publique. À cet égard, elle prend acte que le traitement, qui vise à assurer la sécurité civile sur le territoire national conformément aux dispositions des articles L. 112-1 et L. 112-2 du code de la sécurité intérieure (CSI), s'inscrit dans le cadre du plan de modernisation du système national d'alerte.

En particulier, le traitement projeté doit permettre à ces autorités de déclencher, à distance, une alerte en activant le réseau des sirènes interconnectées *via* l'infrastructure nationale partageable de télécommunication (INPT). La Commission relève que le traitement SAIP doit également permettre de délivrer des informations à la population sur les consignes de sécurité à suivre ainsi que sur l'évolution des événements.

Elle prend acte que le message d'alerte et d'information à la population relatif à ces événements sera également adressé par courrier électronique à des « abonnés », en l'occurrence des fournisseurs de support de communication ayant conclu une convention avec le ministère de l'intérieur, afin que ce message puisse être relayé auprès de la population par différents moyens de communication tels que les automates d'appel des collectivités territoriales, les ondes radio ou encore la télévision.

Compte tenu de ce qui précède, la Commission estime que la finalité poursuivie par le traitement « SAIP » est déterminée, explicite et légitime, conformément aux dispositions de l'article 6-2° de la loi du 6 janvier 1978 modifiée.

Sur la nature des données traitées :

À titre liminaire, la Commission prend acte que les messages d'alerte transmis *via* le traitement projeté ne contiendront aucune données à caractère personnel. À cet égard, seul un message d'alerte et d'information sur les événements en cours et leur évolution, comportant un texte et une copie de carte localisant ledit événement sera délivré.

Dans ce contexte, elle prend également acte qu'aucune donnée sensible au sens de l'article 8 de la loi du 6 janvier 1978 modifiée ne sera collectée et enregistrée dans le traitement. La Commission rappelle que si une modification du traitement était notamment envisagée sur ce point, il reviendrait au ministère d'effectuer une analyse

d'impact relative à la protection des données à caractère personnel conformément aux dispositions de l'article 70-4 de la loi du 6 janvier 1978 modifiée.

La Commission relève par ailleurs que l'utilisation du traitement SAIP est subordonnée à la création d'un compte « utilisateur » par les autorités compétentes afin de déclencher une alerte ou à la création d'un compte « abonné » afin de permettre aux fournisseurs de support de communication de relayer cette alerte à la population.

À ce titre, l'article 2 du projet d'arrêté distingue les données à caractère personnel relatives aux personnes disposant de l'un ou l'autre de ces comptes.

En premier lieu, elle relève que s'agissant des personnes disposant d'un compte « utilisateur », sont collectées les données relatives à :

- leur identification (nom, prénom, adresse postale professionnelle ou personnelle, adresse électronique, numéro de téléphone professionnel ou personnel, numéro identifiant le titulaire d'un certificat électronique (numéro IGC)) ;
- la situation professionnelle de l'utilisateur (qualité ou fonction) ;
- l'identifiant de connexion ainsi qu'au numéro de protocole Internet (« adresse IP »).

En deuxième lieu, la Commission relève que s'agissant des personnes disposant d'un compte « abonné », sont collectées les données relatives à leur identification (adresse électronique, nom et prénom lorsqu'il s'agit d'un abonné personne physique).

Elle relève également que des données se rapportant à la personne physique agissant au nom de l'abonné seront également collectées, à savoir des données relatives à :

- leur identification (nom, prénom, adresse postale professionnelle ou personnelle, adresse électronique, numéros de téléphone professionnel ou personnel) ;
- la situation professionnelle de l'utilisateur (qualité ou fonction).

Interrogé sur le caractère personnel ou professionnel de l'adresse postale, du numéro de téléphone et de l'adresse électronique des personnes concernées, le ministère a indiqué que, par principe, seules les données ayant un caractère professionnel seraient collectées et enregistrées dans le traitement, conformément à la doctrine d'emploi élaborée. Il a néanmoins précisé que la collecte des coordonnées personnelles des utilisateurs disposant d'un compte au traitement « SAIP » pouvait se justifier s'agissant des utilisateurs ne disposant pas de coordonnées professionnelles.

A cet égard, la Commission prend acte que, à sa demande, le projet d'arrêté sera modifié afin de mentionner de manière explicite le caractère professionnel ou, le cas échéant, personnel de chacune des catégories de données précitées.

Dans ces conditions, la Commission estime que les données traitées sont adéquates, pertinentes et non excessives au regard des finalités poursuivies, conformément aux dispositions de l'article 6-3° de la loi du 6 janvier 1978 modifiée.

Sur la durée de conservation :

L'article 4 du projet d'arrêté prévoit que les données relatives aux personnes bénéficiant d'un compte « utilisateur » sont conservées jusqu'à la cessation des fonctions de l'agent titulaire du compte.

La Commission prend acte que cette durée de conservation doit permettre de tenir compte de la durée d'occupation du poste par l'agent amené à utiliser le traitement SAIP, sans que cette durée ne puisse, en tout état de cause, excéder cinq ans à compter de l'enregistrement de ces données.

La Commission rappelle par ailleurs que l'identifiant de connexion et l'adresse IP de l'utilisateur étant des données de traçabilité, leur durée de conservation ne saurait, sauf à justifier de particularités ou de dispositions légales expresses, excéder six mois. Elle prend acte de la modification du projet d'arrêté en ce sens.

En ce qui concerne les données relatives aux personnes disposant d'un compte « abonné », ce même article prévoit que les données ainsi collectées sont conservées cinq ans à compter de leur enregistrement. À cet égard, la Commission prend acte que cette durée correspond à la durée de la convention conclue avec l'abonné, ce qui n'appelle pas d'observation particulière de la Commission.

En tout état de cause, elle rappelle qu'à l'issue des durées de conservation ainsi définies, les données devront être détruites de manière sécurisée.

Compte tenu de ces éléments, la Commission estime que la durée ainsi définie est conforme à l'article 6-5° de la loi du 6 janvier 1978 modifiée.

Sur les personnes habilitées à accéder aux données :

L'article 3 du projet d'arrêté énumère les personnes pouvant accéder, à raison de leurs attributions et dans la limite du besoin d'en connaître, à « *tout ou partie des informations et données* » enregistrées dans le traitement.

La Commission relève que l'ensemble des catégories de personnes énumérées à cet article occupent des fonctions qui justifient qu'elles puissent bénéficier d'un accès à SAIP.

Elle relève en outre que le projet d'arrêté prévoit que les agents de chacun des services mentionnés à cet article feront l'objet de désignations individuelles et d'habilitations spécifiques.

Sur l'information et les droits des personnes :

La Commission prend acte qu'une information sera délivrée aux utilisateurs de SAIP lors de la création de leur profil et que des mentions d'information spécifiques sont prévues dans les conventions conclues entre le ministère de l'intérieur et les abonnés. Elle rappelle qu'il convient pour le ministère de s'assurer que l'information ainsi délivrée soit claire, complète et pédagogique, conformément aux dispositions des articles 70-18 et suivants de la loi du 6 janvier 1978 modifiée.

L'article 6 du projet d'arrêté prévoit que les droits d'accès, de rectification et d'effacement des personnes s'exercent directement auprès de la direction générale de la sécurité civile et de la gestion des crises.

Enfin, ce même article prévoit que le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 modifiée ne s'applique pas au traitement projeté.

À cet égard, la Commission rappelle que, si les dispositions de la directive 2016/680 du 27 avril 2016 susvisée telles que transposées en droit interne, ne mentionnent pas la possibilité pour les personnes concernées de s'opposer au traitement mis en œuvre, les Etats membres conservent, en tout état de cause, la possibilité de prévoir des garanties plus étendues que celles établies dans ladite directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes.

Dans ce contexte, elle considère que l'article 38 précité, qui n'a pas été abrogé par la loi relative à la protection des données personnelles et dont l'application aux traitements relevant de la directive précitée, n'est pas davantage exclu par les dispositions des articles 70-1 et suivants de la loi « Informatique et Libertés », a également vocation à s'appliquer aux traitements relevant du champ d'application de cette directive. Elle relève à cet égard que cet article 38 prévoit la possibilité d'écarter le droit d'opposition lorsque le traitement répond à une obligation légale ou lorsqu'une disposition expresse de l'acte réglementaire autorisant le traitement l'exclut.

En l'espèce, la Commission considère que l'exclusion du droit d'opposition telle que prévue par l'article 6 du projet d'arrêté est strictement proportionnée au regard de la finalité poursuivie par le traitement projeté, à savoir la préservation de la sécurité publique. Compte tenu de ce qui précède, elle estime que la limitation portée à l'exercice du droit d'opposition s'inscrit dans le cadre des dispositions du droit national relatives à la protection des données à caractère personnel et n'est pas de nature à porter une atteinte excessive aux droits et libertés des personnes concernées.

Sur la sécurité des données et la traçabilité des actions :

Le traitement projeté est un service web permettant le relai d'alertes sur des équipements connectés au réseau radio « ANTARES » (réseau numérique des services publics concourant aux missions de sécurité civile) et l'envoi de courriers électroniques à des abonnés au service.

Des armoires de commande permettent la diffusion des alertes sur les équipements de type sirène à partir de boitiers émetteur/récepteur, la Commission relève qu'un chiffrement est mis en œuvre sur ces boitiers réduisant ainsi les risques d'intrusion.

La Commission relève que l'ensemble des équipements en lien avec le service web sont hébergés par le ministère de l'intérieur et que les échanges sont sécurisés au moyen du protocole SSL. En termes de gestion des risques, elle relève que le nombre de postes susceptibles d'accéder au service est de l'ordre de deux cent et que les données à caractère personnel sont pour l'essentiel conservées au sein d'une base de données.

En outre, des profils d'habilitation sont définis, permettant de restreindre les accès autant que de besoin. Pour les utilisateurs reliés au réseau général de transport de l'Etat

(RGT), l'authentification sur le service web nécessite un identifiant personnel, ainsi qu'un mot de passe dont la politique respecte les recommandations de la Commission. Pour les utilisateurs extérieurs au RGT, l'authentification se fait au moyen d'un certificat RGS conservé dans une carte à puce émise par l'Agence Nationale des Titres Sécurisés (ANTS). L'authentification n'appelle donc pas d'observations de la part de la Commission.

Par ailleurs, l'article 5 du projet d'arrêté prévoit que les informations relatives aux opérations de création, consultation, mise à jour et suppression des données sont conservées pendant cinq ans à compter de leur enregistrement. Sur ce point, la Commission estime que, sauf à justifier de particularités ou de dispositions légales expresses, la durée de conservation des traces ne peut excéder six mois. Elle prend acte de la modification du projet d'arrêté en ce sens.

Dans ces conditions, les mesures de sécurité décrites par le ministère sont conformes à l'exigence de sécurité telle que prévue par la loi du 6 janvier 1978 modifiée. La Commission rappelle toutefois que cette obligation nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

Pour la Présidente
Le Vice-Président délégué

Marie-France MAZARS