Délibération n° 2017-031 du 15 mars 2017

de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Contrôle de l'accès aux locaux par le biais d'un dispositif reposant sur la reconnaissance du réseau veineux des doigts de la main* »

présenté par l'Agence Monégasque de Sécurité Numérique

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

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

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par l'Agence Monégasque de Sécurité Numérique le 16 décembre 2016 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle de l'accès aux locaux de l'Agence Monégasque de Sécurité Numérique* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 15 février 2017, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 15 mars 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

L'Agence Monégasque de Sécurité Numérique (A.M.S.N.) est l'Autorité nationale en charge de la sécurité des systèmes d'information, dont les missions sont, entre autres, de prévenir, détecter et traiter les cyberattaques, notamment par la mise en place de conseils, d'une réglementation, de systèmes de détection, de systèmes d'alerte, et d'une capacité de traitement des incidents.

Afin de contrôler l'accès à ses locaux et d'en assurer ainsi la sécurité, cette Agence souhaite mettre en place un dispositif biométrique reposant sur la reconnaissance du réseau veineux des doigts de la main.

Le traitement automatisé d'informations nominatives objet de la présente délibération est soumis à l'avis de la Commission conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le responsable de traitement indique que le traitement a pour finalité « *Contrôle de l'accès aux locaux de l'Agence Monégasque de Sécurité Numérique ».*

Les personnes concernées sont les fonctionnaires et agents de l'Etat.

Enfin, les fonctionnalités sont les suivantes :

- établir une liste d'identifiants ;
- enregistrer des événements ;
- stocker sur un lecteur biométrique le nom et le prénom de l'utilisateur ;
- programmer le dispositif ;
- contrôler les accès ;
- permettre la constitution de preuves en cas d'infractions.

La Commission rappelle toutefois que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* » aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

En l'espèce, la finalité du présent traitement doit être plus explicite c'est-à-dire être claire et précise pour les personnes concernées en indiquant que le contrôle d'accès aux locaux s'exerce par le biais d'un dispositif biométrique reposant sur la reconnaissance du réseau veineux des doigts de la main.

Par conséquent, elle modifie la finalité comme suit : « *Contrôle de l'accès aux locaux par le biais d'un dispositif reposant sur la reconnaissance du réseau veineux des doigts de la main* ».

II. Sur la licéité et la justification du traitement

Le traitement est justifié par le respect d'une obligation légale et par un motif d'intérêt public puisqu'il répond à l'obligation pour le responsable de traitement de prendre toutes mesures utiles, au regard de la nature des données qu'il traite, permettant non seulement de préserver leur sécurité en empêchant, notamment, qu'elles soient déformées ou endommagées mais aussi de veiller à ce qu'elles soient inaccessibles à des tiers non autorisés, au sens de l'article 23 de la Loi n° 1.435 du 8 novembre 2016, de l'article 5 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 et de l'article 18 de la Loi n° 1.430 du 13 juillet 2016.

Il est par ailleurs justifié par la réalisation d'un intérêt légitime poursuivi par le responsable du traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

A cet égard, le responsable de traitement indique que le traitement permet de contrôler l'accès aux locaux de l'A.M.S.N., « *afin de protéger les systèmes d'information et les données contre des actions malveillantes ou des évènements qui pourraient affecter leur intégrité, leur disponibilité, ou leur confidentialité* ».

La Commission constate par ailleurs que les seuls évènements enregistrés sont lorsqu'un utilisateur est accepté par le système, déclenchant ainsi l'ouverture de la porte, et lorsqu'un utilisateur inconnu présente son doigt au lecteur.

Elle note enfin que lorsqu'un utilisateur est supprimé du système, son nom et prénom sont alors supprimés du journal d'évènements.

La Commission considère donc que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité: nom et prénom des personnes concernées ;
- données d'identification électronique : mot de passe (pour les administrateurs du système uniquement) ;
- données biométriques : codage du réseau veineux du doigt ;
- horodatage : date, heure, état de l'utilisateur (accepté ou inconnu), identifiant numérique de l'utilisateur dans le lecteur, nom, prénom.

Ces informations ont pour origine les personnes concernées, à l'exception des informations d'horodatage qui ont pour origine le lecteur biométrique.

La Commission considère ainsi que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

- ***Sur l'information préalable des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée par le biais d'un document spécifique.

Ce document n'ayant pas été joint à la présente demande d'avis, la Commission rappelle que les personnes concernées doivent impérativement être informées de l'identité du responsable de traitement, de la finalité du traitement, de l'identité des destinataires et de l'existence d'un droit d'accès aux informations les concernant.

- ***Sur l'exercice du droit d'accès, de modification et de mise à jour***

Le droit d'accès s'exerce par voie postale. La réponse à ce droit d'accès s'exerce par voie postale ou sur place.

Le délai de réponse à une demande de droit d'accès est de 30 jours.

La Commission constate que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

V. Sur les destinataires et les personnes ayant accès au traitement

- ***Sur les destinataires***

Les informations sont susceptibles d'être communiquées aux Autorités judiciaires ou administratives monégasques.

La Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

Par ailleurs, les lecteurs étant en mode autonome et ne disposant pas de port de communication permettant l'extraction des données, la Commission constate que cette Direction ne pourra prendre connaissance des informations que directement sur les lecteurs biométriques.

La Commission considère que ces transmissions sont conformes aux exigences légales.

- ***Sur les personnes ayant accès au traitement***

Les personnes habilitées à avoir accès au traitement sont :

- les administrateurs du traitement dont s'agit, à savoir le directeur et le directeur-adjoint de l'Agence : tous droits ;
- le prestataire : en maintenance, uniquement sur place et après obtention des droits auprès du directeur ou du directeur-adjoint de l'agence.

A cet égard, le responsable de traitement précise que la possibilité d'accéder au journal d'évènements n'est donnée qu'au directeur, au directeur-adjoint et au prestataire pendant ses interventions.

Il précise en outre qu'il n'est pas possible d'effacer les évènements dans leur globalité ou d'effacer un évènement en particulier et que le système conserve 10.000 évènements de façon cyclique.

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, la Commission considère ainsi que les accès susvisés sont justifiés.

Elle demande toutefois que les accès des administrateurs soient nominatifs et sécurisés par un mot de passe réputé fort.

Par ailleurs, la Commission demande la mise en place d'une journalisation automatisée desdits accès.

En ce qui concerne le prestataire, elle constate que son réseau veineux n'est pas enregistré et qu'il n'accède au système qu'une fois que le mot de passe administrateur a été saisi soit par le directeur, soit par le directeur adjoint.

La Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

VI. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

La Commission rappelle toutefois que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

Par ailleurs, elle rappelle qu'en cas de remplacement, de réparation ou de dépose d'un lecteur, toutes les informations directement et indirectement nominatives contenues dans ce dernier doivent être détruites sur place.

VII. Sur la durée de conservation

Les informations concernant l'identité, les données d'identification électronique et les données biométriques des personnes concernées sont supprimées dès la fin de l'exercice de leurs fonctions.

La Commission en prend acte.

Par ailleurs, le responsable de traitement indique que les informations concernant l'horodatage et les accès sont supprimées dès la fin de l'exercice des fonctions de tout employé ou lors de la survenance du 10.000^{e} évènement sur le lecteur.

A cet égard, la Commission demande que ces informations ne soient pas conservées plus de trois mois.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Contrôle de l'accès aux locaux par le biais d'un dispositif reposant sur la reconnaissance du réseau veineux des doigts de la main* ».

Rappelle que :

- les personnes concernées doivent impérativement être informées de l'identité du responsable de traitement, de la finalité du traitement, de l'identité des destinataires et de l'existence d'un droit d'accès aux informations les concernant ;

- les Services de Police monégasque ne pourront avoir communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- en cas de remplacement, de réparation ou de dépose d'un lecteur, toutes les informations directement et indirectement nominatives contenues dans ce dernier doivent être détruites sur place.

Demande :

- que les accès des administrateurs soient nominatifs et sécurisés par un mot de passe réputé fort ;

- qu'une journalisation automatisée desdits accès soit mise en place ;

- les informations concernant l'horodatage et les accès soient supprimées au bout de trois mois.

Sous réserve de la prise en compte de ce qui précède,

La Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre par l'Agence Monégasque de Sécurité Numérique du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle de l'accès aux locaux par le biais d'un dispositif reposant sur la reconnaissance du réseau veineux des doigts de la main* ».**

Le Président

Guy MAGNAN