Délibération n° 2017-147 du 19 juillet 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 d'accès aux locaux Informatiques et de la Section des Informations Générales des Etudes et du Renseignement (SIGER) par reconnaissance de l'empreinte digitale et du réseau veineux du doigt* »

présenté par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne 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 l'Ordonnance du 23 juin 1902 établissant une Direction de la Sûreté Publique, modifiée ;

Vu l'ordonnance Souveraine n° 765 du 13 novembre 2006 relative à l'organisation et au fonctionnement de la Direction de la Sûreté Publique, modifiée ;

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 la délibération n° 2011-82 du 21 octobre 2011 portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par le Ministre d'Etat, le 8 mai 2017, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Contrôle d'accès aux locaux Informatiques et de la Section des Informations Générales des Etudes et du Renseignement (SIGER) par reconnaissance de l'empreinte digitale et du réseau veineux du doigt* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 6 juillet 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 19 juillet 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Les locaux de la Direction de la Sûreté Publique doivent faire l'objet de mesures de protection en adéquation avec ses missions de sécurité. A cet égard, celle-ci souhaite mettre en place des restrictions d'accès reposant sur un système biométrique relativement à ses locaux les plus sensibles.

Ainsi, le traitement automatisé d'informations nominatives objet de la présente 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 présent traitement a pour finalité « *Contrôle d'accès aux locaux Informatiques et de la Section des Informations Générales des Etudes et du Renseignement (SIGER) par reconnaissance de l'empreinte digitale et du réseau veineux du doigt* ».

Il concerne les agents et fonctionnaires de l'Etat de la Direction de la Sûreté Publique.

Ce traitement a pour fonctionnalités de :

- « *contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation ;*
- *permettre la constitution de preuve en cas d'infraction* ».

Les locaux concernés sont le local informatique et ceux de la Section des informations générales des études et du renseignement (SIGER).

La Commission constate ainsi que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

La Commission relève que la DSP assure des missions de sécurité et tranquillité publiques consacrées aux articles 1-1 a 1-3 de l'ordonnance n° 765 du 13 novembre 2006.

En outre, aux termes de l'article 1er de la Loi 1.430 du 13 juillet 2016, il est rappelé que « *la police a pour objet de veiller à la sécurité nationale* ».

En ce qui concerne le traitement dont s'agit, la DSP dispose de locaux qui doivent nécessairement faire l'objet d'une protection renforcée eu égard aux personnels, aux informations, aux équipements et installations qu'ils hébergent.

Il en va ainsi notamment du local informatique et des locaux de la Section des informations générales des études et du renseignement (SIGER).

Il appert que le présent traitement, permettant un contrôle d'accès biométrique auxdits locaux, correspond à la réalisation d'un intérêt légitime poursuivit par le responsable de traitement.

Toutefois ce contrôle d'accès est effectué par un système biométrique vérifiant à la fois le réseau veineux et l'empreinte digitale des agents et fonctionnaires de la DSP habilités à pénétrer dans les locaux faisant l'objet d'une restriction d'accès.

En ce qui concerne les empreintes digitales, les gabarits sont conservés sur les terminaux d'accès de la DSP, non reliés entre eux. La Commission estime qu'une conservation de cette donnée biométrique sur un support non maîtrisé par la personne concernée (support individuel) accroit les risques relativement à sa vie privée.

Elle relève toutefois qu'en cas de justification particulière fondée sur les caractéristiques spécifiques d'un responsable de traitement, et en respectant une sécurité adéquate et renforcée, cette modalité de conservation peut être envisagée.

La Commission constate qu'en l'espèce, tel est le cas.

En outre, la Commission relève que les données biométriques stockées sur le PC lors de l'enrôlement sont supprimées dès que ce dernier a été effectué.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : nom, prénom ;
- données d'identification électronique : numéro d'identification ;
- données biométriques : empreinte digitale, empreinte veineuse ;
- informations temporelles, horodatage : date et heure d'accès.

Les informations ont pour origine la personne concernée en ce qui concerne l'identité et les données biométriques. Les autres informations proviennent du lecteur.

La Commission relève également que le système enregistre les raisons d'un refus d'accès (utilisateur non reconnu, tentative d'accès hors plage horaire autorisée, etc.). Elle en prend acte.

La Commission considère 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***

L'information préalable des personnes concernées est réalisée à partir d'une circulaire interne accessible en intranet.

Ce document n'ayant pas été joint à la demande, la Commission rappelle que toutes les personnes concernées doivent être informées conformément aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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

Le droit d'accès est exercé sur place auprès du Directeur de la Sûreté Publique.

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

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

La Commission constate qu'il n'y a pas de destinataires des informations objets du présent traitement.

Les accès sont définis comme suit :

- le Chef de la Section des Technologies de la Sécurité ;
- le Chef du Groupe Informatique.

La Commission relève que ces personnes disposent d'un accès administrateur à la solution.

De plus s'agissant des prestataires, 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 leur contrat de prestation de service. En outre, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

La Commission considère que ces accès sont justifiés.

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.

Cependant les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

De plus, la copie ou l'extraction d'informations issues de ce traitement doivent être chiffrées sur son support de réception.

La Commission rappelle enfin 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.

VII. Sur la durée de conservation

Les informations nominatives collectées seront conservées :

- pendant la durée du contrat de travail plus un an en ce qui concerne les informations relatives à l'identité ;
- pendant la durée de l'affectation plus un an en ce qui concerne les données biométriques ;
- 15 jours en ce qui concerne les informations temporelles.

La Commission considère que le délai de conservation des données biométriques est trop long. Elle demande à ce que ces données soient supprimées dès que l'agent cesse ses fonctions ou que son autorisation d'accès aux zones concernées a été retirée.

Après en avoir délibéré, la Commission :

Rappelle que :

- toutes les personnes concernées doivent être informées conformément aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort ;

- la copie ou l'extraction d'informations issues de ce traitement doivent être chiffrées sur son support de réception.

Fixe la suppression des données biométriques à la cessation de fonction de l'agent ou au retrait de son autorisation d'accès aux zones concernées.

Sous le bénéfice 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 le Ministre d'Etat, du traitement automatisé d'informations nominatives ayant pour finalité *« Contrôle d'accès aux locaux Informatiques et de la Section des Informations Générales des Etudes et du Renseignement (SIGER) par reconnaissance de l'empreinte digitale et du réseau veineux du doigt* ».**

Le Président

Guy MAGNAN