Délibération n° 2019-114 du 17 juillet 2019

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

« *Gestion des habilitations et des accès au Système d'information par l'Active Directory* » exploité par la Direction des Réseaux et des Systèmes d'Information

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 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 1er avril 2019, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion des habilitations et des accès au Système d'information par l'Active Directory* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 31 mai 2019, 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 17 juillet 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

L'Administration exploite des systèmes d'information permettant à ses Services de fonctionner relativement aux missions qui leur sont dévolues. Pour autant, les fonctionnaires, agents de l'état, suppléants et prestataires ne doivent pouvoir accéder qu'aux seules informations strictement nécessaires aux postes qu'ils occupent. A cette fin, elle déploie un traitement de gestion des habilitations permettant de gérer l'authentification des utilisateurs à ses systèmes d'information, veillant ainsi à la légitimité de l'accès et participant de ce fait à la sécurité de ces derniers.

Ce dispositif impliquant l'exploitation d'informations nominatives, le Ministre d'Etat soumet le traitement y afférent dont la finalité est la « *Gestion des habilitations et des accès au Système d'information par l'Active Directory* ».

Ainsi, ce dernier 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 « *Gestion des habilitations et des accès au Système d'information par l'Active Directory* ».

Il concerne les fonctionnaires et agents de l'Etat, les suppléants et les prestataires dotés d'un poste de travail.

Les fonctionnalités du traitement sont :

- Gestion des comptes utilisateurs (création, modification, désactivation, suppression) ;
- Gestion des profils et groupes utilisateurs ;
- Gestion des autorisations d'accès aux ressources informatiques (création, modification, suppression) ;
- Gestion de la mobilité et des départs ;
- Gestion des mots de passe temporaires ;
- Gestion de la sécurité des Systèmes d'information (SI) : maitrise des accès aux SI, suivi de la sécurité (anti-virus, malware), mise en place des remontées d'alertes sur les risques d'intrusion, établissement de rapports (ex : audit de sécurité, détection de risques, …) ;
- Etablissement de statistiques, indicateurs et tableaux de bord ;
- Permettre la supervision des accès aux applications (veiller à la journalisation des accès, collecter et enregistrer des évènements systèmes (logs) permettant de tracer les accès des utilisateurs aux applications et données ; établir des alertes et/ou des rapports qui permettent de détecter des risques de malveillance et de s'assurer de la cohérence des accès avec les habilitations délivrées ;
- Disposer, le cas échéant, de preuves en cas d'infractions avec possibilité d'extraction et/ou de copies sur un support distinct protégé en vue d'une communication aux Autorités compétentes habilitées.

La Commission constate 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

Le responsable de traitement indique que le présent traitement est justifié par le respect d'une obligation légale à laquelle il est soumis.

La Commission relève que la mise en place d'un tel outil est nécessaire au fonctionnement sécurisé d'un système d'information et est également justifiée par l'intérêt légitime du responsable de traitement, sans que ne soit méconnus, ni l'intérêt, ni les droits et libertés fondamentaux des personnes concernées.

Il est en outre précisé, en ce qui concerne la justification par une obligation légale, que le traitement doit être conforme à la politique de sécurité des systèmes d'information de l'Etat, annexée à l'Arrêté Ministériel n° 2017-56 du 1er février 2017. Il y est notamment indiqué que :

- « *Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants : besoin d'en connaitre (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès), moindre privilège (chaque utilisateur accède aux ressources minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui)* » ;
- *« Les applications manipulant des données sensibles doivent permettre une gestion fine par profil d'accès. Les principes du besoin d'en connaitre et du moindre privilège s'appliquent. »*
- *« Toute action d'autorisation d'accès d'un utilisateur à une ressource des S.I. doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel ;*
- *Une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui de l'AMSN* ».

Il est indiqué qu'il est également justifié par l'Ordonnance Souveraine n° 7.012 du 20 juillet 2018 portant création de la DRSI, et notamment les dispositions de l'article 2 4), 5), 6) 7), 9) et 11).

Enfin, il est fait référence à la Charte des systèmes d'information de l'Etat annexée à l'Arrêté Ministériel n° 2015-703 du 26 novembre 2015, qui contient en son sein des règles relatives aux accès au SI et à la sécurité de ce dernier.

La Commission considère que ce 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 traitées

Les informations nominatives traitées sont :

- identité : nom, prénom, matricule (optionnel) ;
- adresse et coordonnées : adresse électronique, n° téléphone fixe professionnel ;
- vie professionnelle : société (si prestataire, poste/fonction, département de rattachement (compagnie), hiérarchie (si fonctionnaire), groupe utilisateur affecté, dates de début et de fin de mission pour les prestataires ;
- données d'identification électronique : identifiant utilisateur, mot de passe chiffré ;
- informations temporelles : horodatages, etc. : log de connexion, opération réalisée (création, modification, suppression), ID ;
- identification du demandeur (hiérarchie) : nom, prénom ;
- matrice des responsabilités/actions sur l'AD : nom, prénom, action possible et ressources.

Les informations relatives à l'identité et à la vie professionnelle, en ce qui concerne les personnes en poste au sein de l'Administration, ont pour origine la Direction des Ressources Humaines et de la Formation de la Fonction Publique. Elles ont pour origine le prestataire en cas de personne externe.

En ce qui concerne les adresses et coordonnées elles ont pour origine le centre de service de la DRSI ou le service de maintenance des bâtiments publics. La Commission relève qu'elles ne proviennent pas de ce dernier organisme mais de la Direction des Ressources Humaines et de la Formation de la Fonction Publique.

Les informations relatives aux données d'identification électronique ont pour origine le centre de service DRSI (le mot de passe est choisi par l'utilisateur) et les informations temporelles sont générées par le système.

En outre, relativement à l'identification du demandeur, la Commission constate à l'analyse du dossier que les informations y relatives ont pour origine le traitement d'assistance aux utilisateurs.

Par ailleurs, la Commission relève que le traitement a notamment pour fonctionnalité le suivi de la sécurité (antivirus, malware), ce qui génère *de facto* la collecte d'informations nominatives indirectes telles que les adresses IP et de manière plus générale toutes les informations en relation avec des tentatives de connexion des personnes tierces captées par les outils sécurité. Elle prend donc acte de la collecte, même si elle considère que les personnes potentiellement concernées par celle-ci n'ont pas à faire l'objet d'une information particulière, cela demandant des mesures disproportionnées au regard de l'intérêt de la démarche, comme le prévoit l'article 14 de la Loi n° 1.165, modifiée.

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 par la Charte des systèmes d'information de l'Etat et par le biais d'un document de renseignement.

Toutefois ces documents ne s'analysent pas en une information des personnes concernées au sens de l'article 14 de la Loi n° 1.165 quant à l'exploitation d'un traitement en objet.

Aussi la Commission demande que l'information des personnes concernées soit effectuée conformément à l'article 14 de la loi n° 1.165.

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

Le droit d'accès est exercé par voie postale, courrier électronique ou sur place auprès de la Direction des Réseaux et des Systèmes d'Information.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, la Commission considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

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

La Commission constate que les informations objets du traitement sont susceptibles d'être communiquées aux autorités compétentes en cas de litige.

Les accès sont en outre définis comme suit :

- Gestionnaires AD (4 personnes) : tous droits, dans le cadre de leur mission notamment de maintenance et de gestion des rôles et groupes ;

- Personnel du Centre de Service (5 personnes) : inscription, modification, suppression (hors informations temporelles) ;

- RSSI et gestionnaires de la sécurité à la DRSI : consultation pour les contrôles et audits sécurité ;

- Tout utilisateur du SI : accès en consultation aux informations relatives à l'identité, à l'adresse, à la vie professionnelle (annuaire).

La Commission constate qu'il est fait recours à des prestataires. Elle rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 les droits d'accès de ces derniers doivent être limités à ce qui est strictement nécessaire à l'exécution de leurs contrats de prestation de service. De plus, 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 les rapprochements et les interconnexions avec d'autres traitements

Le responsable de traitement indique que le traitement est interconnecté avec tous les traitements dont les applicatifs qui en ont besoin pour en gérer les habilitations.

Il est également interconnecté avec le traitement ayant pour finalité l'assistance aux utilisateurs, et dont la formalité y afférente doit être soumise à la Commission.

VII. 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, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

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.

VIII. Sur la durée de conservation

Les données sont conservées :

- 90 jours après le départ de l'intéressé en ce qui concerne l'identité, les adresses et coordonnées, la vie professionnelle, les données d'identification électronique, durée qui peut être portée au temps que dure une procédure en cas de litige ;

- un an en ce qui concerne les informations temporelles ;

- un an après le départ de l'utilisateur en ce qui concerne l'identification du demandeur ;

- le temps de l'affectation de la personne en ce qui concerne la matrice des responsabilités/actions sur l'AD.

La Commission considère que ces durées sont conformes aux exigences légales, excepté les durées relatives aux données d'identification électronique et à l'identification du demandeur qu'elle estime disproportionnées en l'absence de justification particulière.

Aussi, elle en fixe leurs durées de conservation :

- à un an à compter de la collecte en ce qui concerne les données relatives à l'identification du demandeur ;

- au départ de la personne concernée en ce qui concerne les données d'identification électronique.

Après en avoir délibéré, la Commission :

Constate que :

- sont collectées par le biais de la fonctionnalité de suivi de la sécurité (antivirus, malware) les adresses IP et de manière plus générale toutes les informations en relation avec des tentatives de connexion des personnes tierces captées par outils sécurité, qui s'analysent en des informations nominatives indirectes ;

- les personnes potentiellement concernées par celle collecte n'ont pas à faire l'objet d'une information particulière, cela demandant des mesures disproportionnées au regard de l'intérêt de la démarche, comme le prévoit l'article 14 de la Loi n° 1.165, modifiée ;

- les informations relatives aux adresses et coordonnées ont pour origine la DRHFPP et celles relatives à l'identification des demandeurs proviennent du traitement ayant pour finalité « *assistance aux utilisateurs* ».

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé ;

Demande que :

- l'information des personnes concernées soit effectuée en conformité avec l'article 14 de la Loi n° 1.165 ;

- le traitement ayant pour finalité « *assistance aux utilisateurs* » lui soit soumis dans les meilleurs délais.

Fixe :

- la durée de conservation des informations relatives à l'identification du demandeur à un an à compter de la collecte ;

- la durée de conservation des informations relatives aux données d'identification électronique au départ de la personne concernée.

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 *« Gestion des habilitations et des accès au Système d'information par l'Active Directory ».***

Le Président

Guy MAGNAN