Délibération n° 2021-080 du 21 avril 2021

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 accès à des environnements spécifiques du SI* »

exploité par la Direction 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 l'Ordonnance Souveraine n° 7.996 du 12 mars 2020 portant création de la Direction des Systèmes d'Information ;

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 14 janvier 2021, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion des accès à des environnements spécifiques du SI* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 11 mars 2021, 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 21 avril 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Afin de renforcer la sécurité de son système d'information et de « *gérer les accès et habilitations des personnes habilitées à avoir accès à des ressources spécifiques* », le Ministre d'Etat souhaite mettre en œuvre le traitement ayant pour finalité la « *Gestion des accès à des environnements spécifiques du SI* ».

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 accès à des environnements spécifiques du SI* ».

Il concerne les fonctionnaires, les agents de l'Etat et les prestataires dotés d'un poste de travail habilités à avoir accès à l'environnement concerné.

Les fonctionnalités du traitement sont :

- « *Validation des habilitations des administrateurs et des utilisateurs ;*
- *Gestion de manière centralisée des accès et permissions sur les systèmes concernés ;*
- *Application des permissions spécifiques à chaque utilisateur en fonction des équipements ;*
- *Traçabilité des actions effectuées sur l'environnement ;*
- *Corrélation avec les alertes remontées du SIEM ;*
- *Gestion des documents de travail des utilisateurs de l'environnement concerné ;*
- *Etablissement de statistiques non nominatives* ».

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, ainsi que par la réalisation d'un intérêt légitime, sans que ne soient méconnus les droits et libertés fondamentaux des personnes concernées.

A cet égard, il précise que le traitement n'a pas pour objet de surveiller les personnes concernées.

La Commission relève que la mise en place d'un tel outil participe à la sécurisation du système d'information, conformément 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 est en outre indiqué qu'il est également justifié par l'Ordonnance Souveraine n° 7.996 du 12 mars 2020 portant création de la DSI, notamment en son point 10 qui dispose que la DSI est chargée « *d'assurer la gestion des annuaires et des contrôles d'accès logiques et physiques* ».

Par ailleurs, la Charte des Systèmes d'information de l'Etat et la Charte Administrateur Réseaux et Systèmes d'Information de l'Etat rappellent aux utilisateurs du SI et aux administrateurs leurs obligations en termes de sécurité. Les Administrateurs sont à cet égard sensibilisés à leur fonction dotée de prérogatives renforcées, à la qualité des actions qu'ils doivent mener, tant en matière de confidentialité que de besoin de traçabilité.

Il est enfin précisé qu'assurer la sécurité des Systèmes d'Informations est une « *obligation professionnelle* » qui s'applique aux fonctionnaires et agents de l'Etat en application de l'article 58 de l'Ordonnance Souveraine n° 3.413 du 29 aout 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, et rappelée à l'article premier de l'Arrêté n° 2017-56, susvisé.

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, UPN ;
- adresses et coordonnées : email ;
- données d'identification électronique : login et mot de passe de l'administrateur ;
- informations temporelles : horodatage (jour, heure, minute, seconde des actions réalisées) ;
- profil : groupe utilisateur, droits affectés à la personne ou au groupe dans lequel la personne est intégrée ;
- log de connexion : adresse IP de connexion, login, UPN, machine, horodatage, connexion/déconnexion, action effectuée, tentative d'accès, catégorie de sévérité.

Les profils sont créés suite aux demandes de création ou modification de comptes reçues *via* le Centre de Service.

Les informations relatives à l'identité et aux adresses, ont pour origine la DSI lorsqu'elle habilite ses personnels au traitement.

Enfin, excepté le mot de passe fourni par l'utilisateur, les autres informations sont générées par le système.

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 le biais de l'Intranet de l'Administration.

La Commission relève que la mention concernée, jointe au dossier, est conforme aux dispositions légales.

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

Le droit d'accès est exercé par voie postale auprès de la Direction 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.

Elle relève également de la mention jointe au dossier que le droit d'accès peut s'effectuer par voie électronique.

Aussi, 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.

Sous cette réserve, elle 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, modifiée.

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

Le responsable de traitement indique que les informations objets du traitement sont susceptibles d'être communiquées à « *toute autorité agissant dans le cadre de ses fonctions juridictionnelles* ».

Par ailleurs, ont accès au traitement dans le cadre de leurs missions les agents habilités de la DSI et toute personne travaillant sous son autorité, dans le cadre de leurs missions d'administration, d'assistance technique et de maintenance.

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 les traitements légalement mis en œuvre suivants :

- « *Gestion des habilitations et des accès au Système d'information* », afin de disposer des éléments permettant d'identifier les accès au SI ;
- « *Gestion et analyse des évènements du système d'information* » afin de veiller à la traçabilité et à la sécurité des actions effectuées sur le réseau ;
- «*Gestion des accès à distance au système d'information du Gouvernement* », à des fins de sécurisation d'accès distants.

Il est également rapproché avec le traitement légalement mis en œuvre ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DSI* », aux fins de recueillir les demandes en lien avec le traitement.

La Commission constate que ces interconnexions et ce rapprochement sont conformes aux exigences légales et aux finalités initiales pour lesquelles les informations nominatives ont été collectées.

Elle tient cependant à rappeler que les interconnexions de traitements ne doivent pas conduire à créer une surveillance précise, continue et inopportune des utilisateurs du SI.

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.

De plus la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée 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.

VIII. Sur la durée de conservation

Les données relatives aux informations temporelles et aux logs de connexion sont conservées deux semaines.

Les autres informations sont conservées tant que l'utilisateur est habilité à avoir accès à l'environnement.

La Commission estime toutefois que la durée de conservation de deux semaines n'est pas suffisante pour permettre d'identifier en cas de problème ce qui a pu se produire sur les systèmes concernés et fixe donc leur durée de conservation à 3 mois.

Après en avoir délibéré, la Commission :

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 ;

- la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception ;

- les interconnexions de traitements ne doivent pas conduire à créer une surveillance précise, continue et inopportune des utilisateurs du SI.

Fixe la durée de conservation des données relatives aux informations temporelles et aux logs de connexion à trois mois.

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 accès à des environnements spécifiques du SI ».***

Le Président

Guy MAGNAN