Délibération n° 2019-136 du 18 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 accès à distance au Système d'information du Gouvernement* »,

dénommé « *Le Bastion* »

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 7 juin 2019, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion des accès à distance au Système d'information du Gouvernement* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 5 aout 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 18 septembre 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. Par délibération 2019-114, la Commission a émis un avis favorable au traitement ayant pour finalité « *Gestion des habilitations et des accès au Système d'information par l'Active Directory* », qui permet la gestion des habilitations auxdits systèmes relativement aux personnels autorisés.

Afin de maîtriser l'ensemble des accès aux ressources de l'Administration, le Ministre d'Etat souhaite également soumettre le traitement ayant pour finalité « *Gestion des accès à distance au Système d'information du Gouvernement* », qui a pour objectif d'« *assurer la sécurité des accès à distance au Système d'information du Gouvernement par le biais d'une solution adaptée en évitant le recours à des logiciels de prise en main à distance non sécurisés et non maîtrisés* ».

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 distance au Système d'information du Gouvernement* ».

Il est dénommé « *Le Bastion* ».

Il concerne les fonctionnaires et agents de l'Etat, ainsi que les prestataires avec accès à distance.

Les fonctionnalités du traitement sont :

- Permettre un accès à distance à certains environnements précis et restreints du système d'information du Gouvernement de manière sécurisée ;
- Disposer d'informations sur les prestataires permettant d'examiner les demandes, d'implémenter la procédure et son fonctionnement ;
- Assurer l'implémentation de la solution, son activation, sa désactivation et sa suppression ;
- Assurer la gestion de l'AD - Active Directory – spécifique au bastion et gérer les comptes associés ;
- Analyser les besoins de maintenance de la solution et communiquer avec les personnes intéressées en cas d'intervention sur le Bastion (ex. maintenance) ;
- Permettre la traçabilité des sessions et l'imputabilité des actions ;
- Vérifier, a posteriori, si nécessaire, les actions réalisées par les utilisateurs de la solution et disposer, le cas échéant, de preuves ou de débuts de preuves si de besoin ;
- Conserver des éléments retraçant la réalisation des opérations réalisées par les agents à des fins, le cas échéant, de vérification et de compréhension d'une situation donnée ;
- Assurer les opérations de suivi et de maintenance des équipements et ressources du Bastion ;

- Etablir des statistiques, rapports d'évaluation et d'analyse.

Il est précisé que les accès aux applications, environnements, logiciels, etc., sont gérés par les logs dédiés desdits environnements, applications, logiciels, etc.

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 et la réalisation d'un intérêt légitime, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission relève que la mise en place d'un tel outil résulte des attributions conférées à la DRSI, qui doit assurer la disponibilité des ressources informatiques en environnement sécurisé, conformément aux dispositions de l'Ordonnance n° 7.012 du 20 juillet 2018 qui porte création de celle-ci.

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 (PSSIE), annexée à l'Arrêté Ministériel n° 2017-56 du 1er février 2017. S'il ne s'agit pas directement d'une obligation légale imposant la mise en œuvre du présent traitement, la prise en compte de manière obligatoire de la PSSIE dans l'élaboration et l'utilisation du Bastion participe nécessairement à sa sécurité. La PSSIE impose notamment des obligations procédurales dans la gestion et révocation de droits d'accès aux systèmes d'information, la gestion des privilèges, etc.

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, et à la Charte « *Administrateur réseaux et système d'information de l'Etat* », qui imposent aux utilisateurs et admirateurs des systèmes d'Information de l'Etat des obligations propres à leurs fonctions.

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 :

En ce qui concerne les référents du service demandeur :

- identité : nom, prénom ;
- coordonnées professionnelles : téléphone, email ;
- vie professionnelle : fonction, service ;
- informations relatives à la demande : projet, raison de l'accès, date de début, date de fin, date de validation, commentaires ;
- statut de la demande : production/en attente/clôturée/refusée avec raison.

En ce qui concerne le prestataire signataire de la convention :

- identité du signataire : nom, prénom ;
- vie professionnelle : fonction, signature, société;
- statut : date de la convention.

En ce qui concerne la personne désignée pour accéder à distance :

- identité : nom, prénom ;
- vie professionnelle : société ou entité, fonction ;
- coordonnées professionnelles : email, téléphone, adresse postale, email autre pour des informations sur les opérations de maintenance ;
- données d'identification électronique : login, mot de passe ;
- données de connexion : serveur, lieu et adresse IP publique depuis laquelle le/les prestataires devront ouvrir la connexion (IP de l'entreprise ou du domicile) ;
- connaissance de la solution : oui/non (explication orale si réponse négative) ;
- objet de la demande : horaire de connexion, date (début-fin), raison de l'accès, intitulé du projet/logiciel/mission concerné(e) ;
- logs de connexion sur le réseau (pare-feu/environnement/équipement interne réseau/serveur cible interne) : données d'horodatage de la dernière connexion (date et heure), DN de l'utilisation (sur serveur cible, prénom, nm, login, adresse IP de connexion (pare-feu) ;
- éléments de la solution Wallix : DN de l'utilisation ; enregistrement des sessions (vidéo des actions réalisées par la personne) ;
- profil utilisateur/plateforme Wallix : nom, prénom.

En ce qui concerne le contact/référent chez le prestataire (si autre que précédent) :

- identité : nom, prénom ;
- coordonnées professionnelles : email.

En ce qui concerne les Agents de la DRSI en charge du projet (référent interne) :

- identité : nom, prénom ;
- coordonnées professionnelles : téléphone, email ;
- vie professionnelle : fonction, service.

Les informations ont pour origine la personne concernée, le prestataire ou le référent du service demandeur pour tout ce qui concerne les informations préalables permettant d'identifier la personne introduisant une demande et la personne concernée par la demande.

Le suivi de la demande est effectué par l'Agent de la Division Sécurité.

En outre, en ce qui concerne les Agents de la DRSI en charge du projet, les informations ont pour origine l'Agent en charge des demandes.

Enfin, toutes les données liées à la traçabilité, l'horodatage, ou aux éléments de la solution Wallix sont générées par le système.

Toutefois, la Commission constate à l'analyse du dossier que les informations relatives à la génération d'une demande (personne effectuant la demande/personne concernée) ont pour origine le traitement d'assistance aux utilisateurs, qui est le canal conduisant à la création d'un profil.

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 une mention sur le document de collecte ou une mention dans la convention.

Toutefois ces documents ne sont pas joints à la demande d'avis.

Aussi la Commission rappelle que l'information des personnes concernées doit être 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 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.

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 :

- RSSI : tout accès dans le cadre de ses missions de validation et de contrôle ;
- Administrateurs de la cellule sécurité de la DRSI : tout accès ;
- Administrateurs des divisions infra et réseaux : communication des données permettant le paramétrage des serveurs via les tickets d'intervention GLPI ;
- Agents du Centre de Service chargés de la gestion des comptes AD : communication des données permettant de valider la procédure de création d'un compte AD.

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 rapproché avec les traitements suivants :

- Gestion des techniques automatisées de communication, légalement mis en œuvre, pour permettre l'échange de messages entre intervenants ;
- Assistance aux utilisateurs par le Centre de Service de la DRSI, non légalement mis en œuvre, « *pour permettre d'une part aux demandeurs de suivre l'évolution du traitement de la demande par la cellule sécurité, d'autre part aux intervenants d'intervenir le moment venu dans la procédure* » ;
- Gestion de la messagerie professionnelle (exchange), en cours d'analyse, pour permettre l'échange de messages entre intervenants ;
- Gestion de la messagerie professionnelle (O365), en cours d'analyse par la Commission, pour permettre l'échange de messages entre intervenants ;
- Gestion des habilitations et des accès au Système d'information par l'Active Directory, légalement mis en œuvre. Ce rapprochement n'est pas nécessaire afin d'habiliter les utilisateurs au présent traitement, qui dispose de ses propres habilitations. Il sert cependant à ce que l'utilisateur externe qui a passé l'étape du Bastion soit reconnu ensuite par le Système d'information de l'Etat.

Concernant le traitement ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DRSI* », la Commission demande qu'il lui soit soumis dans les meilleurs délais.

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, il est recommandé que toute extraction/duplication d'informations en lien avec ledit traitement (au format CSV, Excel ou autres) créée à des fins de manipulation, de gestion de données, soit sécurisée sur un support/application (format) choisi réputé fort.

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 « *tant que l'accès au Bastion est opérationnel + 12 mois* », excepté les informations relatives aux logs de connexion, aux éléments de la solution Wallix, et à l'horodatage qui sont conservées 12 mois glissants.

La Commission considère que ces durées sont conformes aux exigences légales, excepté les durées relatives aux l'identité des référents du service demandeur.

Aussi, elle en fixe leurs durées de conservation à un an à compter de la collecte.

Enfin, elle relève qu'il n'est pas prévu de durée de conservation des demandes ayant fait l'objet d'un refus. Aussi, elle fixe le délai de conservation de ces informations à 6 mois à compter du refus.

Après en avoir délibéré, la Commission :

Constate que les informations relatives à la génération d'une demande (personne effectuant la demande/personne concernée) ont pour origine le traitement ayant pour finalité « *assistance aux utilisateurs* ».

Rappelle que :

- l'information des personnes concernées doit être effectuée conformément à l'article 14 de la Loi n° 1.165 ;

- 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 ;

Recommande que toute extraction/duplication d'informations en lien avec ledit traitement (au format CSV, Excel ou autres) créée à des fins de manipulation, de gestion de données, soit sécurisée sur un support/application (format) choisi réputé fort.

Demande que le traitement ayant pour finalité « *assistance aux utilisateurs par le Centre de Service de la DRSI* » lui soit soumis dans les meilleurs délais.

Fixe :

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

- la durée de conservation des demandes ayant fait l'objet d'un refus à 6 mois à compter du refus.

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 distance du Système d'Information du Gouvernement ».***

Le Président

Guy MAGNAN