Délibération n° 2020-124 du 16 septembre 2020

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 centralisée des accès aux applications du SI*»

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 15 juin 2020, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion centralisée des accès* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 13 aout 2020, 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 16 septembre 2020 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Afin de « *simplifier l'expérience utilisateur du système d'information (SI) du Gouvernement tout en veillant à la sécurité du SI* », le Ministre d'Etat souhaite mettre en œuvre le traitement ayant pour finalité la « *Gestion centralisée des accès* ».

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 centralisée des accès* ».

Il concerne les fonctionnaires et agents de l'Etat, les prestataires dotés d'un poste de travail, ainsi que les utilisateurs des applications éligibles.

Les fonctionnalités du traitement sont :

- Validation des habilitations des utilisateurs ;
- Sécurisation de l'accès aux applications éligibles ;
- Validation ou refus d'accès au SI ;
- Visualisation par les utilisateurs des applications auxquelles ils ont accès ;
- Suivi des accès des utilisateurs et analyse des logs de connexion à des fins de sécurité du SI ;
- Gestion des alertes ;
- Etablissement de statistiques.

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 qu'il s'agit d'accès logiques.

Par conséquent, elle modifie la finalité comme suit : « *Gestion centralisée des accès aux applications du SI* ».

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.

La Commission relève que la mise en place d'un tel outil participe à la sécurisation 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 notamment 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 est indiqué qu'il est également justifié par l'Ordonnance Souveraine n° 7.996 du 12 mars 2020 portant création de la DSI.

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 ;
- adresse et coordonnées email, adresse professionnelle, n° de téléphone ;
- vie professionnelle : poste, fonction, département, service, groupe utilisateur ;
- données d'identification électronique : login, mot de passe ;
- informations temporelles : horodatages, etc. : horodatage : jour, heure, minute des actions ;
- jetons de connexion : identifiant AD, attributs nécessaire au fonctionnement de l'application cible ;
- log de connexion : adresse IP de connexion, login, nom, prénom, type d'utilisateur (user ou admin), device, localisation du point de connexion (pays et ville), navigateur et OS utilisés, horodatage, statut de connexion, tentative d'accès, sévérité.

Les informations relatives à l'identité aux coordonnées et à la vie professionnelle ont pour origine le traitement légalement mis en œuvre ayant pour finalité « *Gestion des habilitations et des accès au Système d'information* ».

Excepté le mot de passe fourni par l'utilisateur, les autres informations 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.

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 d'un document spécifique.

Ce dernier n'étant pas joint au dossier, la Commission rappelle que l'information des personnes concernées doit être conforme aux dispositions de l'article 14 de la Loi n° 1.165, modifiée.

➢ *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.

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 :

- Administrateurs du Gouvernement habilités : tous droits, dans le cadre de leur mission notamment de maintenance et de gestion des rôles et groupes ;

- Utilisateurs du Gouvernement : accès aux applications.

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* » ;
- « *Gestion des accès à distance au système d'information du Gouvernement* » ;
- « *Sécurisation des accès à distance au SI pour les flottes nomades BYOD et professionnelles* » ;
- « *Gestion de la messagerie professionnelle* 0365».

A l'analyse des éléments du dossier, ces interconnexions sont conformes aux finalités initiales.

Il est également rapproché 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 :

- Tant que l'utilisateur est habilité à avoir accès à au moins une application cible en ce qui concerne les informations relatives à l'identité, aux adresses et coordonnées, à la vie professionnelle et au login. ;

- 3 mois en ce qui concerne les informations temporelles et les logs de connexion ;

- 5 jours en ce qui concerne les jetons de connexion.

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

Après en avoir délibéré, la Commission :

Modifie la finalité comme suit : « *Gestion centralisée des accès aux applications du SI*».

Rappelle que :

- les personnes concernées doivent être informées de manière conforme 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, 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 le traitement ayant pour finalité « *assistance aux utilisateurs par le centre de service de la DSI* » lui soit soumis dans les meilleurs délais ;

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 centralisée des accès aux applications du SI ».***

Le Président

Guy MAGNAN