Délibération n° 2020-126 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 et analyse des évènements du système 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 la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

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 l'Ordonnance Souveraine n° 7.680 du 16 septembre 2019 portant application de l'article 25 de la Loi n° 1.435 relative à la lutte contre la criminalité technologique, 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 15 juin 2020, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion et analyse des évènements du système d'information* » ;

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 renforcer et rationnaliser la sécurité de son système d'information, le Ministre d'Etat souhaite mettre en œuvre le traitement ayant pour finalité « *Gestion et analyse des évènements du système d'information* ».

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 et analyse des évènements du système d'information* ».

Il concerne tout utilisateur du Système d'information de l'Etat et les personnels habilités à avoir accès au traitement.

Les fonctionnalités du traitement sont :

- « *Mettre en place une plateforme de gestion de logs transverses ;*
- *Collecter les évènements ou log de connexion des ressources identifiées du système d'information (SI) ;*
- *Analyser des logs ;*
- *Etablir des reportings, tableaux de bord et indicateurs de sécurité selon les besoins identifiés ;*
- *Mettre en place un SIEM (Détection d'évènements de sécurité) ;*
- *Assurer le suivi des équipements du système d'information ;*
- *Disposer d'une visibilité du SI et de son fonctionnement ;*
- *Disposer d'éléments permettant de comprendre les ralentissements ou dysfonctionnements ;*
- *Disposer de critères support des actions de prévention, correction, évolution du SI du Gouvernement ;*
- *Mettre en place des mesures d'alerte ;*
- *Veiller à la qualité des actions des administrateurs ;*
- *Conserver les logs conformément à la PSSIE, aux impératifs de sécurité de SI, et le cas échéant, dans le cadre de contentieux* ».

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.

La Commission relève que la mise en place d'un tel outil participe à la sécurisation du 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. A cet égard, le responsable de traitement précise qu'il ne s'agit pas de surveiller ou de contrôler de manière systématique et permanente les activités des personnes physiques sur le Système d'information.

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.

Par ailleurs, la Charte Administrateur Réseaux et Systèmes d'Information de l'Etat rappelle aux administrateurs « *que toute action sur les systèmes d'information de l'État fait l'objet d'une journalisation permettant son imputabilité* ». De plus, il est également prévu, en ce qui concerne les modalités de contrôle, que « *L'Administrateur peut procéder à des contrôles dans le cadre de sa mission (surveillance et détection d'anomalies sur les réseaux et systèmes d'information). Lesdits contrôles doivent être effectués conformément aux exigences suivantes :*

- *tous les contrôles sont non nominatifs ;*
- *lorsque ces contrôles permettent de déceler une anomalie ou un dysfonctionnement, l'Administrateur peut alors effectuer des vérifications complémentaires plus approfondies (liste des émetteurs ou destinataires des données, contenu des messages professionnels, etc.). Si ces vérifications permettent d'identifier formellement une personne en charge, l'Administrateur informe cette dernière et lui demande de prendre les mesures de correction nécessaires, en lui proposant son aide* ».

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 : personnes habilitées à avoir accès au traitement : nom, prénom ;
- vie professionnelle : personnes habilitées à avoir accès au traitement : fonction, habilitations ;
- données d'identification électronique : personnes habilitées à avoir accès au traitement : login, mot de passe ;
- log de connexion : login utilisateur, nom du poste, adresse MAC, type d'action effectuée/refusée sur la ressource loguée, action effectuée sur le poste de travail, données d'horodatage (date, heure précise), durée de l'action, applications exécutées, les évènements (ex ; Event source, event ID, event destination).

Les informations relatives à l'identité et à la vie professionnelle ont pour origine la Direction de la DSI qui habilite ses personnels au traitement.

Excepté le mot de passe fourni par l'utilisateur, les autres informations sont générées par le système et les ressources du SI intégrées.

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 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 administratives ou judiciaires agissant dans le cadre de leurs missions.

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

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.

Toutefois, il appert de l'analyse du dossier que les informations objets du traitement sont transmises à l'AMSN à des fins de stockage. La Commission s'interroge sur la durée de conservation effective des données auprès de l'AMSN, le responsable de traitement indiquant qu'il existe des durées de conservation différenciées en fonction de l'objectif du stockage.

En tout état de cause, elle estime que l'AMSN est, en l'espèce, en mesure de lire les données transmises à tout moment et en dehors d'alertes avérées. Or l'AMSN ne peut, en application de l'article 25 de la Loi n° 1.435 relative à la lutte contre la criminalité technologique et de son Ordonnance Souveraine n° 7.680 d'application, qu'intervenir *a posteriori* aux seules fins de caractériser une attaque sur les Systèmes d'Information de l'Etat, et ne peut pas, en application de l'article 27 de ladite Loi, procéder elle-même à la sécurisation du SI qui doit être effectuée par « *des prestataires de services qualifiés en matière de sécurité de système d'information* » agréés par ses soins.

Aussi, elle exclut la transmission des informations à l'AMSN.

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* ».

Cependant, il appert à la lecture du dossier les interconnexions suivantes :

- *« Gestion centralisée des accès » ;*
- « *Gestion de la politique de filtrage des accès internet* ».

Ces interconnexions sont conformes aux finalités initiales.

Il est également indiqué que peut être interconnecté « *tout traitement reposant sur des équipements intégrés dans le périmètre* » du présent traitement d'analyse.

A cet égard, la Commission rappelle que ces interconnexions ne doivent pas introduire de surveillance permanente et systématique 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.

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 :

- 12 mois après le départ de la personne habilitée en ce qui concerne ses informations relatives à l'identité et à la vie professionnelle. ;
- 12 mois glissants en ce qui concerne les logs de connexion ;
- tant que l'agent est habilité à avoir accès en ce qui concerne les données d'identification électronique.

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

Après en avoir délibéré, la Commission :

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 ;

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

Exclut la transmission des informations à l'AMSN.

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 et analyse des évènements du système d'information ».***

Le Président

Guy MAGNAN