Délibération n° 2021-079 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

« *Traçabilité des évènements d'annuaires et des accès aux ressources associées* »

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 « *Traçabilité des évènements d'annuaires et des accès aux ressources associées* » ;

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 « *monitorer les actions effectuées sur le système* », le Ministre d'Etat souhaite mettre en œuvre le traitement ayant pour finalité la « *Traçabilité des évènements d'annuaires et des accès aux ressources associées* ».

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 « *Traçabilité des évènements d'annuaires et des accès aux ressources associées* ».

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

Les fonctionnalités du traitement sont :

- « *Conserver les traces des accès et actions effectués sur les environnements cibles ;*
- *Effectuer, sur demande, des remontées sur des évènements ;*
- *Retrouver, sur demande, les actions réalisées sur un document, un fichier, un serveur de fichier (ex. suppression, modification, changement de répertoire) ;*
- *Mettre en place des alertes destinées à suivre des actions spécifiques à des fins d'administration des ressources et de sécurité du SI ;*
- *Etablir des statistiques et rapports nominatifs ou non en lien avec les opérations précitées ;*
- *Détecter, alerter et permettre de réaliser des remontées sur des accès et/ou des actions non autorisés (à des données nominatives ou non) ;*
- *Permettre de disposer d'un début de preuve en cas d'infraction aux règles internes à l'Administration ou aux règles de droit commun, notamment d'actes relevant d'infractions sanctionnées par le Code Pénal* ».

La Commission constate la possibilité d'établir des statistiques nominatives. Elle relève également que si le traitement n'a pas pour objectif de contrôler les personnes, un profil d'utilisation attendu de la personne concernée est créé, alertant en cas de différence significative entre le comportement attendu et le comportement effectif.

Elle demande donc que les paramétrages, les statistiques nominatives et le contrôle individuel qui peut en découler soient précisément évalués afin que la vie privée des utilisateurs soit respectée.

Elle rappelle de plus que le présent traitement ne doit pas conduire à une surveillance permanente et inopportune des personnes concernées.

Sous ces réserves, 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.

La Commission relève que la mise en place d'un tel outil participe à la sécurisation du système d'information, conformément la politique de sécurité des systèmes d'information de l'Etat, annexée à l'Arrêté Ministériel n° 2017-56 du 1er février 2017, notamment en ses points 21, 23, 25 et 35.

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, initiales, ID ;
- adresses et coordonnées : email ;
- vie professionnelle : statut (utilisateur, administrateur) ;
- données d'identification électronique : login et mot de passe de l'administrateur ;
- informations temporelles : date des actions (jour, mois, année), heure, minute, seconde ;
- droits des utilisateurs du SI : groupe, action ;
- évènements enregistrés : date de l'évènement, origine de l'évènement (user, compte service, serveur …), objet de l'évènement, action (déplacé, supprimé, modifié, ouvert).

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

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

La Commission constate qu'eu égard aux fonctionnalités de preuve à des fins pénales, les informations objets du traitement sont susceptibles d'être communiquées aux Autorités administratives ou judiciaires agissant dans le cadre de leurs missions.

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, avec des droits adaptés au besoin d'en connaitre des fonctions qui interviennent sur le présent traitement.

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 ;

ainsi qu'avec tout traitement identifié comme devant être intégré aux mesures de sécurité du présent traitement.

Il est également rapproché avec les traitements légalement mis en œuvre suivants :

- « *Assistance aux utilisateurs par le Centre de Service de la DSI* », aux fins de recueillir les demandes en lien avec le traitement ;
- « *Gestion de la messagerie professionnelle* », aux fins d'échanges et rapports entre les intervenants.

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

Elle rappelle toutefois 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, pares-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.

En outre, il convient de préciser que 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 sont conservées 12 mois glissants excepté en ce qui concerne les données d'identification électronique qui sont conservées tant que l'administrateur est habilité à avoir accès au traitement.

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

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.

Demande que les paramétrages, les statistiques nominatives et le contrôle individuel qui peut en découler soient précisément évalués afin que la vie privée des utilisateurs soit respectée.

Rappelle que :

- le présent traitement ne doit pas conduire à une surveillance permanente et inopportune des personnes concernées ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pares-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 ;

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

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 *« Traçabilité des évènements d'annuaires et des accès aux ressources associées ».***

Le Président

Guy MAGNAN