

Délibération n° 2024-151 du 26 juillet 2024

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 du réseau informatique du Gouvernement* »

exploité par la Direction des Systèmes d'Information

et 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 l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'administration et l'administré, modifiée, et ses textes d'application ;

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 9 avril 2024, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion du réseau informatique du Gouvernement* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 6 juin 2024, 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 26 juillet 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Direction des Systèmes d'Information veille au maintien en condition opérationnelle et en condition de sécurité du système d'information, support des activités des Services de l'Etat, par la mise en place de mesures techniques et organisationnelles.

A cet égard, les ressources (équipements) et applications systèmes / logicielles génèrent des logs lorsqu'un événement (voire une connexion) se produit dans l'équipement ou l'application. Ces mesures passent notamment par la gestion des réseaux (supports des flux de données) qui relèvent de procédures spécifiques telles que la gestion des logs de connexions de tout utilisateur et administrateur.

Le fonctionnement de ces ressources implique l'exploitation de données sur les utilisateurs et administrateurs, données qui permettent de les identifier (ex. nom, prénom, matricule) ou de les rendre identifiables.

Ainsi, le traitement y afférent 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 du réseau informatique du Gouvernement* ».

Il concerne les fonctionnaires et agents de l'Etat, les prestataires et les utilisateurs du réseau.

Les fonctionnalités du traitement sont :

- administrer les ressources et le réseau du Gouvernement ;
- optimiser le fonctionnement et les fonctions du réseau ;
- assurer le transport dynamique et sécurisé des flux réseaux des ressources du Gouvernement ;
- gérer les alertes sur les équipements et recevoir des notifications ;
- superviser les équipements réseaux ;
- identifier les personnes habilitées à intervenir sur les ressources ;
- établir des statistiques (non nominatives) sur le comportement des équipements.

La Commission considère donc que le traitement est licite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165, modifiée.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le présent traitement est justifié par un motif d'intérêt public 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 est précisé que « *Le traitement répond par ailleurs à un intérêt légitime du responsable de traitement de veiller à la mise à disposition d'outils répondant aux besoins des métiers, aux attentes des utilisateurs et à la sécurité du SI et des réseaux* ».

La Commission constate surtout, en lieu et place d'un motif d'intérêt public, que le présent traitement relève d'une obligation légale, qui s'infère du nécessaire respect de la politique de sécurité des systèmes d'information de l'Etat (PSSIE), annexée à l'Arrêté Ministériel n° 2017-56 du 1^{er} février 2017 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'administration et l'administré, modifiée, et dans le respect des Chartes applicables à l'Administration, dont la Charte administrateurs réseaux et systèmes d'information annexée à l'Arrêté Ministériel n° 2018-281 du 4 avril 2018 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'administration et l'administré, modifiée.

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 des administrateurs des ressources ;
- données d'identification électronique : login et mot de passe de l'administrateur de la solution ;
- informations temporelles : flux selon la ressource (numéro de port et protocole, username, adresse IP, adresse MAC, hostname, domaine utilisateur, SSI de l'équipement, requête, données, état de la session, email, parfois nom prénom) ;
- logs des actions effectuées par les administrateurs : adresse IP, actions réalisées, données d'horodatage, adresse IP des devices gérés.

L'origine des informations n'appelle pas d'observations.

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 internes à l'Administration est réalisée par l'inscription du traitement sur la liste des traitements mis en œuvre par la Direction des Systèmes d'Information diffusée sur l'Intranet du Gouvernement. La Commission constate que la mention y relative 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 ou par le biais d'un formulaire dédié auprès de la Délégation Interministérielle chargée de la Transition Numérique.

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.

La Commission constate 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

S'il est indiqué que l'utilisation des informations objets du traitement demeure « interne », la Commission constate à la lecture de la mention d'information portée à l'attention des personnes concernées, qu'elles sont susceptibles d'être communiquées aux Autorités administratives ou judiciaires agissant dans le cadre de leurs missions.

Par ailleurs, ont un accès tous droits au traitement les administrateurs réseaux habilités de la DSI.

En outre, 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 permettre l'accès à la solution ;
- « *Gestion des accès dédiés au Système d'information du Gouvernement* » afin d'assurer la sécurité des accès au SI ;
- « *Gestion et analyse des événements du Système d'Information* » afin de veiller à la traçabilité, à la sécurité des actions effectuées sur l'environnement, l'établissement de statistiques et d'alertes le cas échéant ;
- « *Supervision des équipements* » afin de permettre l'envoi d'alertes ;
- « *Gestion de la politique de filtrage des accès à Internet* » pour la récupération des logs des proxy envoyés par le traitement « *Gestion et analyse des événements du Système d'Information* ».

Il est également rapproché avec le traitement légalement mis en œuvre ayant pour finalité la « *Gestion de la messagerie professionnelle* », afin de recevoir, selon les solutions, des rapports de supervision des équipements.

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.

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 relatives à l'identité et aux données d'identification électronique sont conservées « *tant que l'utilisateur a accès aux ressources ou à la solution* » tandis que les informations temporelles et les logs des actions effectuées par les administrateurs sont conservées 30 jours maximum.

S'agissant des logs, la Commission relève qu'ils sont « *réutilisés* » dans le traitement ayant pour finalité « *Gestion et analyse des événements du système d'information* » et considère que leur durée de conservation y est étendue au sein dudit traitement selon les modalités définies ayant reçu un avis favorable de sa part.

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

Après en avoir délibéré, la Commission :

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.

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 du réseau informatique du Gouvernement* ».**

Le Président

Robert CHANAS