Délibération n° 2020-125 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 de la politique de filtrage des accès à Internet* »

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° 5.840 du 13 mai 2016 portant création du Secrétariat Général du Gouvernement ;

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 de la politique de filtrage des accès à Internet* » ;

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 d'éviter que les accès Internet délivrés aux utilisateurs des systèmes d'information du Gouvernement permettent la consultation de sites en compromettant la sécurité ou proposant des contenus illicites, le Ministre d'Etat souhaite mettre en œuvre le traitement ayant pour finalité la « *Gestion de la politique de filtrage des accès à Internet* ».

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 de la politique de filtrage des accès à Internet* ».

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

Les fonctionnalités du traitement sont :

- « *Filtrer les accès / les flux à Internet dans le respect de la politique de filtrage de l'Etat ;*
- *Gérer les profils utilisateurs concernant les accès à Internet ;*
- *Sécuriser des accès et prévenir des risques d'atteinte au SI par l'authentification des utilisateurs ;*
- *Prévenir l'accès (accidentel ou volontaire) à des sites ou contenus considérés comme illicites ou non conformes à la politique de filtrage ;*
- *Disposer d'un début de preuve, le cas échéant, en cas d'infraction ou d'acte susceptible de constituer des infractions à la règlementation ;*
- *Etablir des statistiques* ».

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 que le traitement « *n'a pas pour objectif de surveiller ou contrôler l'activité professionnelle des utilisateurs* » et que les statistiques sont effectuées « *à des fins techniques et de fonctionnement, dans le cadre des fonctionnalités listées dans les formulaires, non à des fins de surveillance des personnes* ».

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, et qu'il s'intègre aux missions du Secrétariat Général du Gouvernement qui doit mettre à dispositions des Services des outils à utiliser dans les meilleurs conditions ; en l'espèce, l'outil Internet doit être utilisé en prévenant l'accès à des sites illicites ou compromettant la sécurité du Système d'Information.

La Commission relève par ailleurs que la Charte utilisateur des systèmes d'information de l'Etat contient en son sein des dispositions relatives à l'utilisation d'Internet.

De plus, les administrateurs sont informés par la Charte Administrateur Réseaux et Systèmes d'Information de l'Etat, 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 : utilisateur : nom, prénom ;
- vie professionnelle : utilisateur : profil (groupe), département ;
- données d'identification électronique : login, mot de passe ;
- informations temporelles : date, heure de consultation ;
- log de connexion : adresse IP (privée et publique) du terminal, groupe LDAP, localisation du terminal, politique de filtrage appliquée (générique ou spécifique), information du poste (mac adress, numéro, OS, modèle du terminal), information de l'applicatif (version…), type d'accès, action de filtrage (autorisé, bloqué), ressource consultée (URL), ressource(s) de rebond (équipement de sortie) ;
- identification des administrateurs : nom, login, mail, rôle, scope, mot de passe (chiffré), droits ;
- commentaires : le cas échéant, observation liée au fonctionnement de la solution.

En ce qui concerne la rubrique commentaire, la Commission rappelle que son contenu doit être encadré, proportionné, et strictement en lien avec l'objectif recherché.

Les informations relatives à l'identité, à la vie professionnelle, aux données d'identification électronique et à l'identification des administrateurs ont pour origine le système d'authentification.

Les informations temporelles et les logs de connexion sont générés par le système.

Enfin, les commentaires sont renseignés par les administrateurs.

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.

La Commission constate néanmoins, sans que cela puisse se substituer à l'information telle que prévue à l'article 14 de la Loi n° 1.165, susvisée, que la Charte des systèmes d'information de l'Etat dispose en son point 2.2.4.1. « Internet / Intranet » « *L'accès à des applications en ligne (sites web, web Radio, web TV, blogs, forums, chats, applications existantes ou à venir etc.) est strictement réservé à un usage professionnel. L'utilisateur ne doit en aucune manière se livrer à la consultation, au chargement, téléchargement, au stockage, à la publication ou à la diffusion de fichiers, y compris vidéos ou musicaux, et de messages électroniques, dont le contenu présente un caractère injurieux, diffamatoire, pornographique ou raciste etc. et ce sans que cette liste ne soit exhaustive, sauf dans le cadre d'une mission liée à la recherche et à la poursuite d'infractions. Ceci s'applique tant aux fichiers qu'aux messages électroniques, avec ou sans pièces attachées et à toute forme de communication quelle que soit la forme des contenus (sonores, audiovisuels, multimédias ou logiciel). L'utilisation des réseaux sociaux peut être source de risques et de responsabilité notamment en termes de sécurité et/ou d'image pour l'Administration. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées* ».

- ***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 le responsable de traitement, s'il indique ne communiquer aucune information à des destinataires, entend conserver les éléments infractionnels constatés sur son SI. Aussi, elle estime que les informations objets du traitement sont susceptibles d'être communiquées aux Autorités administratives ou judiciaires agissant dans le cadre de leurs missions légalement conférées.

Par ailleurs, le traitement est administré par les agents habilités de la DSI et de la DDUN.

La Commission relève que de plus en plus de traitements métiers ou de téléservices font l'objet d'interventions de Directions supports qui administrent ou créent les solutions. Ces Directions supports sont décrites comme disposant d'accès aux traitements concernés. La Commission rappelle que ces dernières n'ont pas à avoir accès en continu à l'information métier, dont la sensibilité peut varier en fonction des Services concernés. Elle demande donc

que les accès soient restreints au strict besoin d'en connaitre et que les interventions de supports soient effectuées selon des modalités définies conformes aux règles de l'art.

Elle constate de plus qu'il est fait recours à des prestataires, et 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 concomitamment soumis suivants :

- « *Gestion centralisée des accès* » ;
- « *Gestion et analyse des évènements du système d'information* ».

En outre, la Commission relève qu'il est rapproché avec les traitements de messageries professionnelles, légalement mis en œuvre.

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 Internet en ce qui concerne ses informations relatives à l'identité et à la vie professionnelle. ;

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

- Tant que l'agent est habilité à avoir accès à la solution en ce qui concerne les données d'identification électronique et l'identification des administrateurs ;

- Jusqu'à résolution du dysfonctionnement ou tant que nécessaire à la finalité en ce qui concerne les commentaires.

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 Directions supports n'ont pas à avoir accès en continu à l'information métier dont la sensibilité peut varier en fonction des Services concernés ;

- 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 commentaires doivent être proportionnés à la finalité recherchée et strictement encadrés.

Demande que les accès des Directions supports soient restreints au strict besoin d'en connaitre et que les interventions de supports soient effectuées selon des modalités définies conformes aux règles de l'art.

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 de la politique de filtrage des accès à Internet ».***

Le Président

Guy MAGNAN