Délibération n° 2021-224 du 20 octobre 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

« *Gestion des habilitations au système informatique du Conseil National* »

présenté par le Président du Conseil National

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe du 4 novembre 1950, et notamment son article 10 ;

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 et son protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° 771 du 25 juillet 1964 sur l'organisation et le fonctionnement du Conseil National, 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, susvisée ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par le Président du Conseil National le 8 juillet 2021 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations au système informatique du Conseil National* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 5 septembre 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 20 octobre 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Le Conseil National est une Institution publique consacrée par la Constitution, ainsi que par la Loi n° 771 du 25 juillet 1964, susvisée.

Ses Services relèvent de l'autorité hiérarchique du Président du Conseil National, dont le fonctionnement est défini par un Règlement Intérieur soumis au contrôle du Tribunal Suprême.

Ainsi, le Conseil National revêt le statut d'Autorité publique au sens de l'article 7 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives.

Afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions, le Conseil National souhaite définir des profils d'habilitation dans son système informatique (SI) en séparant les tâches et les domaines de responsabilité.

Ledit traitement, objet de la présente délibération, est donc soumis à l'avis de la Commission conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Gestion des habilitations au système informatique du Conseil National* ».

Les personnes concernées sont toutes les personnes qui se connectent au système informatique du Conseil National.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

- gestion des autorisations d'accès aux ressources informatiques (création, modification, désactivation, suppression) ;
- gestion des comptes utilisateurs et des groupes utilisateurs (création, modification, désactivation, suppression) ;
- gestion des mobilités internes et externes (mutations internes/modifications, départs ou mutations externes/radiation) ;
- gestion des mots de passe réputés forts (mot de passe provisoire et réinitialisation des mots de passe, mais aucune lisibilité des mots de passe utilisateurs par l'administrateur du système informatique) ;
- gestion des points de contrôle et de sécurité (SI) : maîtrise des accès au SI, suivi de la sécurité (anti-virus, malware, anti-spam), remontées d'alertes sur les risques d'intrusion et établissement de rapports (audit de sécurité, détection de risques….) ;
- établissement des données chiffrées quantitatives et nominatives des ressources informatiques ;
- supervision des accès aux applications : journalisation des accès, collecte et enregistrement des évènements système (logs) pour une traçabilité des accès utilisateurs aux applications et aux données ;
- établissement des rapports relatifs aux risques de malveillance et assurer la cohérence des habilitations délivrées avec les accès effectifs ;
- récolte des données nécessaires à l'établissement des éléments de preuves d'infractions possibles ;

- extractions et copies possibles sur un support distinct protégé desdites données en prévision d'une demande de communication aux services de police et aux autorités administratives et judiciaires compétentes.

Au vu de ce qui précède, la Commission considère donc que le 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.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement est justifié par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnait ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

A cet égard, la Commission prend acte que « *Le Conseil National traite l'ensemble des informations nécessaires à la mise en place, au bon fonctionnement et à la sécurisation de son système d'habilitation informatique* ».

Elle relève ainsi que « *L'objectif poursuivi est de sécuriser les informations par nature confidentielles que l'institution a la charge de gérer* ».

Le responsable de traitement précise en outre que « *Le Conseil National le fait dans le respect des droits et libertés fondamentaux de ses utilisateurs* ».

Au vu de ce qui précède, la Commission considère donc que le 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 traitées sont les suivantes :

- identité : prénom, nom, service, fonction ;
- données d'identification électronique : login et mot de passe chiffré ;
- informations temporelles : horodatage, logs de connexion, opération réalisées (création, modification, suppression), ID dates, postes de travail et objet de l'évènement, fichiers journaux quotidiens avec Mac adresse et adresse IP ;
- compte utilisateur : nom du compte, domaine du compte, groupe d'utilisateurs, type de droits, fichier des ressources humaines (service, grade ou fonction, appartenance à un annuaire ou un ou des groupes spécifiques), statut (fonctionnaire, contractuel, suppléant, stagiaire), degrés d'habilitation hiérarchique ou de confidentialité, et selon des dates de début et de fin de mission.

Les informations relatives à l'identité, aux données d'identification électronique et au compte utilisateur ont pour origine soit le fichier des ressources humaines du Conseil National soit sont renseignées par la personne elle-même.

Par ailleurs, les informations temporelles sont générées par le système informatique.

La Commission considère ainsi 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***

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée par le biais de « *La charte informatique du Conseil National* ».

Ce document n'ayant pas été joint à la demande, la Commission rappelle que celui-ci doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993.

- ***Sur l'exercice du droit d'accès***

Le responsable de traitement indique que le droit d'accès s'exerce par courrier électronique auprès du Secrétaire Général du Conseil National.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit intervenir dans le mois suivant la réception de la demande.

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.

La Commission considère 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 du 23 décembre 1993.

V. Sur les destinataires et les personnes ayant accès au traitement

- ***Sur les destinataires***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique et aux Autorités administratives dans le cadre de leurs missions légalement conférées.

La Commission estime ainsi que la communication à la Direction de la Sûreté Publique peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ladite direction ne pourra avoir accès aux informations objet du traitement, que dans le strict cadre de ses missions légalement conférées.

Sous ces conditions, elle considère donc que de telles transmissions sont conformes aux exigences légales.

- ***Sur les personnes ayant accès au traitement***

Les personnes habilitées à avoir accès au traitement sont :

- le responsable informatique et son assistant : tous droits ;
- les prestataires informatiques : tous droits dans le cadre de leurs opérations de maintenance.

Considérant les attributions de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

En ce qui concerne les prestataires, la Commission rappelle toutefois que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat 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.

VI. Sur les rapprochements et les interconnexions

Le responsable de traitement indique que le présent traitement est interconnecté avec tous les traitements déjà mis en œuvre et à venir.

La Commission en prend acte et considère que ces interconnexions sont conformes aux exigences légales.

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'observations particulières.

La Commission constate que les ports non utilisés sont désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur sont protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

La Commission rappelle que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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 les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité, les données d'identification électronique et les données liées au compte utilisateur sont conservées tant que la personne est en poste.

Par ailleurs, les informations temporelles sont conservées 1 an.

La Commission considère donc 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.

Rappelle que :

- l'information des personnes concernées doit être conforme à l'article 14 de la Loi n° 1.165, ainsi qu'à l'article 80 bis de la Loi n° 839 ;

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

- la Direction de la Sûreté Publique ne peut avoir accès aux informations objet du traitement que dans le strict cadre de ses missions légalement conférées.

A la condition 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 Président du Conseil National, du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations au système informatique du Conseil National* ».**

Le Président

Guy MAGNAN