Délibération n° 2023-095 du 21 juin 2023

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 et accès sécurisés aux environnements de l'infrastructure IOT* »

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 1er mars 2023, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion des accès sécurisés à l'infrastructure IOT* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 27 avril 2023, 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 juin 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Le Gouvernement souhaite sécuriser l'accès, la maintenance, la traçabilité et l'imputabilité en lien avec l'infrastructure IOT qu'il utilise. Pour ce faire, il souhaite mettre en œuvre un traitement qui permet d'habiliter les personnes concernées et d'en gérer les accès.

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 des accès sécurisés à l'infrastructure IOT* ».

Il concerne les fonctionnaires et agents de l'Etat et les prestataires agissant pour le compte du Gouvernement avec accès à distance.

Les fonctionnalités du traitement sont :

- enrôlement des utilisateurs par demande du chef de service à la Division exploitation de la DSI ;
- permettre un accès sécurisé et ciblé aux environnements et équipements IOT ;
- disposer d'informations permettant d'examiner les demandes d'accès, d'implémenter la procédure et son fonctionnement ;
- assurer la gestion d'un annuaire spécifique et gérer les comptes associés ;
- analyser les besoins de maintenance de la solution et communiquer avec les personnes intéressées en cas d'intervention sur l'infrastructure IOT (ex. maintenance) ;
- permettre la traçabilité des sessions et l'imputabilité des actions ;
- conserver des éléments retraçant la réalisation des opérations réalisées par les agents à des fins, le cas échéant, de vérification et de compréhension d'une situation donnée ;
- assurer les opérations de suivi et de maintenance des équipements et ressources de l'environnement ;
- établir des statistiques, rapports d'évaluation et d'analyse.

La Commission rappelle toutefois que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* » aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

En l'espèce, la finalité du présent traitement doit être plus explicite en indiquant qu'il s'agit également d'une procédure d'habilitation à l'infrastructure IOT se trouvant dans des environnements du SI du Gouvernement.

Par conséquent, elle modifie la finalité comme suit : « *Gestion des habilitations et accès sécurisés aux environnements de l'infrastructure IOT* ».

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 est précisé que « *Le traitement se justifie par l'intérêt légitime du responsable de traitement d'assurer la sécurité des systèmes d'information et des réseaux utilisés dans le cadre de ses missions, des missions des entités administratives relevant de son autorité* ».

En ce qui concerne l'obligation légale, si la Commission constate qu'elle découle « *par exemple, de ses missions telles que définies, par l'Ordonnance Souveraine n° 7.996 du 12 mars 2020 portant création de la Direction des Systèmes d'Information (DSI), de la PSSIE, et des règles fixées par l'AMSN* », la Commission rappelle qu'aucune obligation légale n'impose la mise en œuvre d'un traitement proposant la présente finalité.

Elle relève néanmoins qu'« *aux termes de l'article 2 chiffre 4 de l'OS n° 7.96, la DSI a pour mission de « procéder à l'étude et au suivi des mises en œuvre des applications informatiques nécessaires au bon fonctionnement des services administratifs en étroite collaboration avec la Direction des Services Numériques et la Direction des Plateformes et des Ressources Numériques »* ».

La Commission relève que la mise en place d'un tel outil participe à la sécurisation système d'information, conformément à la politique de sécurité des systèmes d'information de l'Etat (PSSIE), annexée à l'Arrêté Ministériel n° 2017-56 du 1er février 2017.

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, en ce qui concerne les référents du service demandeur :

- identité : nom, prénom ;
- vie professionnelle : fonction, service ;
- coordonnées professionnelles : téléphone, email ;
- informations relatives à la demande : projet, raisons de l'accès, date de début, date de fin, date de validation, commentaires ;
- statut de la demande : production, en attente, clôturée, refusée avec raison.

Les informations collectées en lien avec les prestataires signataires de la convention :

- identité du signataire : nom, prénom ;
- vie professionnelle : fonction, signature, société ;
- statut : date de la convention.

Les informations nominatives traitées quant aux personnes désignées pour accéder à l'infrastructure IOT :

- identité : nom, prénom ;
- vie professionnelle : société ou entité, fonction ;
- coordonnées professionnelles : téléphone, email, adresse postale ;
- données d'identification électronique : login, mot de passe ;
- données de connexion : serveur, lieu et adresse IP publique depuis laquelle le/les prestataires devront ouvrir la connexion (IP de l'entreprise ou du domicile) ;
- objet de la demande (logiciel, projet, mission) : horaire de connexion, date (début-fin), raison de l'accès, intitulé du projet/logiciel/mission concernée ;
- logs de connexion sur le réseau (pare-feu/environnement/équipement interne réseau/serveur cible interne) : données d'horodatage de la dernière connexion (date,

heure), DN de l'utilisation (sur serveur cible ou machine concernée, prénom, nom, login, adresse IP de connexion (pare-feu) ;
- profil utilisateur/plateforme : nom, prénom, rôles et droits.

Les informations collectées en lien avec les contacts/référents chez le prestataire :

- identité: nom, prénom ;
- coordonnées : email.

Les informations collectées relativement aux agents de la DSI intervenant dans la procédure :

- identité: nom, prénom, signature ;
- vie professionnelle : fonction ;
- suivi de la demande : statut, validation, commentaires ;
- horodatage : date et heure de création et de mise à jour des documents.

Les informations collectées relativement aux agents de la DSI en charge du projet (référent interne) :

- identité: nom, prénom, signature ;
- coordonnées professionnelles : email, téléphone ;
- vie professionnelle : fonction, service.

Sont communiquées par la personne concernée elle-même les informations relatives au prestataire signataire de la convention, celles relatives à l'identité, à la vie professionnelle et au suivi de la demande des agents de la DSI intervenant dans la procédure, ainsi que les informations d'identité, de vie professionnelle, de coordonnées, de données d'identification électronique de la personne désignée pour accéder à l'infrastructure IOT. Il est précisé qu'en ce qui concerne cette dernière catégorie de personnes, lesdites informations peuvent être communiquées par le prestataire ou par la DSI.

Sont produites par le système les informations relatives aux logs sur le réseau, aux éléments de la solution, au profil utilisateur/plateforme et à l'horodatage.

Les informations relatives aux référents du service demandeur sont renseignées par ces derniers, excepté le statut de la demande qui relève de l'Agent de la Division Sécurité.

L'objet de la demande concernant la personne désignée pour accéder à l'infrastructure IOT émane du référent du service demandeur.

Enfin, les informations de contact du prestataire sont communiquées par ce dernier tandis que les informations relatives aux agents de la DSI en charge du projet émanent de l'agent en charge des demandes.

Par ailleurs, en ce qui concerne les commentaires et les raisons du refus d'une demande, la Commission rappelle que leur contenu doit être objectif et la responsabilité de la qualité de ces derniers, notamment en ce qui concerne l'absence de données interdites au sens de l'article 12 de la Loi n° 1.165 ou de propos injurieux, appartient au responsable de traitement.

Sous cette réserve, 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, soit l'outil de communication interne de l'Administration pour les documents se rapportant au fonctionnement de l'Administration* ». La Commission constate que la mention y relative est conforme aux dispositions légales.

Il est en outre précisé que les prestataires sont informés via un mail adressé préalablement à leur accès et au moyen d'une mention portée sur le formulaire de demande d'accès distant. La Commission relève que la mention concernée, jointe au dossier, est conforme aux dispositions légales, à l'exception de l'absence d'information quant à l'éventuelle communication des donnés objets du traitement aux autorités administratives et judiciaires, dont bénéficient les personnes concernées internes à l'Administration. Elle rappelle enfin que le responsable de traitement doit s'assurer que les salariés des prestataires sont individuellement informés de leurs droits.

➢ *Sur l'exercice du droit d'accès, de modification et de mise à jour*

Le droit d'accès est exercé par voie postale, par courrier électronique ou par le biais d'un formulaire en ligne 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.

S'agissant de l'exercice du droit d'accès par voie électronique, la Commission rappelle qu'une procédure doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agit effectivement de 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 à la lecture de la mention d'information portée à l'attention des personnes concernées, que 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 :

- les personnels habilités de la DSI, administrateurs de la solution : tous accès ;
- le Responsable Sécurité des Systèmes d'Information : accès en consultation pour avis.

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.

Elle rappelle également que les règles d'accès des administrateurs doivent être conformes à celles décrites dans la délibération n° 2021-171 relative à la « *Gestion des accès dédiés au Système d'information* » afin de permettre la traçabilité et l'imputabilité des actions que ledit traitement assure.

Sous ces réserves, 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 :

- « *Traçabilité des évènements d'annuaires et des accès aux ressources associées* » ;
- « *Gestion des accès dédiés au Système d'information du Gouvernement* ».

Il est également rapproché avec le traitement légalement mis en œuvre ayant pour finalité la « *Gestion de la messagerie professionnelle* ».

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.

Enfin, il est précisé que « *tout traitement concerné par des accès à distance aux plateformes IIOT nécessiteront une authentification en passant par le présent traitement* ».

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'accès est opérationnel + 12 mois* » excepté les données de logs de connexion sur le réseau et les données d'horodatage qui sont conservées 12 mois glissants.

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

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion des habilitations et accès sécurisés aux environnements de l'infrastructure IOT ».*

Considère une procédure relative au droit d'accès par voie électronique doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agit effectivement de la personne concernée par les informations.

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 ;

- le responsable de traitement doit s'assurer que les salariés des prestataires sont individuellement informés de leurs droits ;

- les règles d'accès des administrateurs doivent être conformes à celles décrites dans la délibération n° 2021-171 relative à la « *Gestion des accès dédiés au Système d'information* » afin de permettre la traçabilité et l'imputabilité des actions que ledit traitement assure ;

- le responsable de traitement doit s'assurer du caractère proportionné des informations portées dans les rubriques commentaires.

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 des habilitations et accès sécurisés aux environnements de l'infrastructure IOT».***

Le Président

Guy MAGNAN