Délibération n° 2021-047 du 17 mars 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 accès physiques au Centre de Service par badges nominatifs* »

exploité par la Direction des Systèmes d'Information (DSI) présenté par le Ministre d'Etat

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 ;

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° 7.996 du 12 mars 2020 portant création de la Direction des Systèmes d'Information ;

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'Arrêté Ministériel n° 2017-56 du 1er 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 son annexe « *Politique de Sécurité des Systèmes d'Information de l'Etat* » ;

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 Ministre d'Etat le 10 décembre 2020 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des accès physiques au Centre de Service » ;*

Vu la prorogation du délai d'examen de ladite demande d'avis notifiée au responsable de traitement le 8 février 2021, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 17 mars 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

L'Administration Gouvernementale souhaite mettre en place des badges nominatifs afin de gérer les accès physiques à la zone d'activité du Centre de Service de la Direction des Systèmes d'Information (DSI) ou aux ressources dédiées au Gouvernement au sein des locaux d'un prestataire.

Le traitement automatisé d'informations nominatives 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.

I. Sur la finalité et les fonctionnalités du traitement

Le responsable de traitement indique que le traitement a pour finalité « *Gestion des accès physiques au Centre de Service ».*

Les personnes concernées sont les « *Personnes habilitées à avoir accès au CDS* ». A cet égard, la Commission constate que sont ainsi concernés les agents et fonctionnaires de la DSI ainsi que les agents du prestataire agissant pour le compte et sur instruction de la DSI.

Enfin, les fonctionnalités sont les suivantes :

- maîtriser les entrées et sorties des locaux dédiés au Centre de Service (CDS) ;
- maîtriser l'accès aux locaux/zones identifiés comme faisant l'objet d'une restriction de circulation justifiée par l'activité des personnes qui y travaillent ou la protection des équipements qui y sont localisés ;
- prévenir l'accès et la circulation de personnes non autorisées ou non habilitées selon les zones identifiées ;
- gérer les badges d'accès (création, suspension, suppression) et des accès associés ;
- établir les documents nécessaires à la gestion des badges (ex. Liste des personnes autorisées à pénétrer dans chaque zone) ;
- établir des statistiques, reporting, tableaux de bord ;
- conserver une trace des accès aux locaux/ zones réservés au CDS ;
- permettre, le cas échéant, la constitution de preuves en cas d'infraction, d'effraction, d'actes malveillants.

La Commission prend acte des précisions du responsable de traitement selon lesquelles les statistiques seront anonymisées.

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 c'est-à-dire être claire et précise pour les personnes concernées en indiquant que les accès physiques se font par un système de badges nominatifs.

Par conséquent, elle modifie la finalité comme suit : « *Gestion des accès physiques au Centre de Service par badges nominatifs* ».

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 s'inscrit dans les missions de la DSI telles que prévues à l'article 2 de l'Ordonnance Souveraine n° 7.996 du 12 mars 2020 portant création de cette dernière, qui dispose notamment qu'elle doit assurer « *le maintien en conditions opérationnelles et en conditions de sécurité du système d'information de l'Administration* », « *fournir des outils de travail modernes au personnel de l'administration* » et assurer la gestion « *des contrôles d'accès logiques et physiques* ».

Le responsable de traitement précise par ailleurs que le traitement s'inscrit dans le cadre de l'application de mesures physiques demandées par la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSI), annexée à l'Arrêté Ministériel n° 2017-56 du 1er février 2017.

La Commission constate ainsi que le traitement dont s'agit répond notamment aux objectifs suivants de cette PSSI :

- *« Objectif 9 : Sécurité physique des locaux abritant les systèmes d'information : Inscrire la sécurisation physique des systèmes d'information dans la sécurisation physique des locaux et dans les processus associés.*

- *Objectif 10 : Sécurité physique des centres informatiques : Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités.*

- *Objectif 11 : Sécurité du système d'information en sûreté : Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site* ».

Le responsable de traitement indique en outre que ce traitement va permettre de « *limiter la possibilité d'accès à certains locaux aux seules personnes autorisées, de protéger des accès de « personnes non habilitées », comme des personnes non affectées à la DSI ou n'agissant pas sous son autorité, plus généralement non autorisés par elle à avoir accès aux locaux, de limiter les accès physiques aux environnements de travail et aux ressources informatiques du Gouvernement Princier* ».

Au vu de ce qui précède, 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 nominatives traitées

Les informations nominatives traitées sont :

- identité : user (statut de la personne) et numéro d'intégration dans la base, nom, prénom, trigramme (trois premières lettres du nom), signature ;
- vie professionnelle : service, fonction/qualité, entité/entreprise ;
- informations temporelles ou horodatage : date et heure d'entrée, date et heure de sortie pour les zones à accès restreint ;
- accès aux locaux : identification des zones autorisées et niveau d'accès ;
- suivi administratif : date de remise du badge, date de restitution, date de début et de fin de validité, date et motif de déclaration de perte/vol ;
- données d'identification : numéro de badge ou de la carte d'accès ;
- logs des lecteurs : données d'horodatage, numéro de badge, identification des lecteurs ;
- données d'identification électronique administrateur : login, mot de passe ;
- logs de connexion administrateur : IP, données d'horodatage, identifiant de l'administrateur.

Les informations relatives à l'identité et à la vie professionnelle ont pour origine le Service Manager de la DSI pour les personnes affectées au CDS et le chef de division pour les intervenants techniques.

Les informations temporelles, les accès aux locaux, les logs des lecteurs et les logs de connexion administrateur ont pour origine le système.

Le suivi administratif a pour origine la DSI (en charge de l'établissement des badges) et la personne concernée.

Les données d'identification ont pour origine la DSI (en charge de l'établissement des badges).

Enfin, les données d'identification électronique administrateur ont pour origine le manager pour le login et la personne concernée pour le mot de passe.

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*

L'information préalable des personnes concernées est effectuée par le biais d'une mention sur le document de collecte, à savoir le formulaire de remise de badge.

A l'analyse de ce document, la Commission considère que celui-ci est conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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

Le droit d'accès s'exerce 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.

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

- ***Sur les destinataires***

Le responsable de traitement indique que toute Autorité administrative et judiciaire dans le cadre de ses missions peut être destinataire des informations.

A cet égard, la Commission prend acte des précisions du responsable de traitement selon lesquelles il s'agit « *de toute autorité judiciaire, administrative ou policière habilitée en droit interne à ordonner, autoriser ou entreprendre l'exécution de procédures de collecte ou de production d'éléments de preuve se rapportant à des enquêtes ou procédures qui peut être destinataire d'informations issues du présent traitement, dans le cadre des missions qui leur sont légalement ou réglementairement conférées et des garanties mises en place conformément au droit interne* ».

La Commission considère donc que ces transmissions sont conformes aux exigences légales.

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

Les personnes habilitées à avoir accès au traitement sont :

- le gestionnaire des badges (DSI) : lecture/consultation, création, modification/mise à jour et suppression ;
- les administrateurs de l'application : lecture/consultation, création et modification/mise à jour ;
- les auditeurs : lecture/consultation ;
- le personnel du prestataire en charge de la maintenance matériel/logiciel : accès à des fins de maintenance.

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

En ce qui concerne le prestataire, elle rappelle 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 son contrat de prestation de service. De plus, ledit prestataire est 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 interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec un traitement ayant pour finalité « *Gestion des habilitations et des accès au Système d'Information par l'Active Directory » et* d'un rapprochement avec un traitement ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DSI* »

La Commission prend acte que ces traitements ont été légalement mis en œuvre et considère que cette interconnexion et ce rapprochement 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'observation particulière.

La Commission rappelle néanmoins 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.

Elle rappelle que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception, conformément à la délibération n° 2010-13 du 3 mai 2010.

La Commission rappelle également 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

Le responsable de traitement indique que les informations relatives à l'identité et à la vie professionnelle ainsi que les données d'identification sont conservées tant que la personne travaille au CDS + 12 mois après la restitution du badge.

Les informations temporelles ou horodatage et les accès aux locaux sont conservés 12 mois.

Le suivi administratif est conservé 12 mois après la restitution du badge.

Les logs des lecteurs et les logs de connexion administrateur sont conservés 12 mois glissant.

Enfin les données d'identification électronique administrateur sont conservées tant que la personne est habilitée à effectuer ces tâches.

A cet égard, la Commission prend acte des précisions du responsable de traitement selon lesquelles ces durées sont liées aux obligations de traçabilité des actions sur le Système d'information et aux impératifs de sécurité entourant le fonctionnement du SI du Gouvernement, tel qu'entendu par les points 4.10.43 et 4.10.45 de la PSSIE.

Elle considère donc que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion des accès physiques au Centre de Service par badges nominatifs* ».

Rappelle que :

- la réponse au droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort ;

- la copie et 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 « *Gestion des accès physiques au Centre de Service par badges nominatifs* ».**

Le Président

Guy MAGNAN