Délibération n° 2021-049 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 par badge aux locaux de l'Administration* »

exploité par la Direction des Systèmes d'Information (DSI) présentée 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 24 décembre 2020 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des accès physiques par badge aux locaux de l'Administration » ;*

Vu la prorogation du délai d'examen de ladite demande d'avis notifiée au responsable de traitement le 19 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 ses bâtiments et locaux à l'intérieur des bâtiments dotés d'un contrôle d'accès.

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

Ce traitement a pour finalité « *Gestion des accès physiques par badge aux locaux de l'Administration ».*

Les personnes concernées sont les « *Fonctionnaires et Agents de l'Etat* » et les « *Prestataires (si besoin identifiés)* ».

Enfin, les fonctionnalités sont les suivantes :

- maîtriser les entrées et sorties des locaux ;
- maîtriser l'accès à certains locaux, certaines zones identifiées comme faisant l'objet d'une restriction de circulation, liée à l'activité des personnes qui y travaillent – et à la confidentialité des données qu'elles traitent – ou la protection des équipements qui y sont localisés ;
- canaliser l'accès des visiteurs ;
- prévenir l'accès à la circulation de personnes non autorisées ou non habilitées selon les zones et les horaires identifiés ;
- établir des statistiques, reporting, tableaux de bord ;
- permettre, le cas échéant, la constitution de preuves en cas d'infraction.

La Commission prend acte des précisions du responsable de traitement selon lesquelles un badge temporaire est attribué à tout visiteur à l'entrée et récupéré à la sortie mais que celui-ci est « *totalement anonyme (banalisé) sans information relative à la personne* ».

Elle note également que « *Les statistiques sont uniquement une quantification de masse (nombre, moyenne,…)* ».

La Commission constate ainsi 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 prend ainsi acte des précisions du responsable de traitement selon lesquelles le traitement dont s'agit « *s'appuie sur les missions et compétences de 2 Directions de l'Administration :*

- *La DRHFFP [Direction des Ressources Humaines et de la Formation de la Fonction Publique] qui est en charge de l'application des dispositions relatives aux statuts des fonctionnaires de l'Etat et des dispositions concernant les agents non titulaires, notamment, des mesures relatives aux conditions de travail.*
  Le système permet de limiter l'accès aux locaux selon des horaires déterminés par les besoins du Service et modulables selon la fonction des personnes concernées connue par la DRHFFP. Aussi cette Direction gère les aspects du traitement relatifs à la gestion des données portant sur les accès (ex. identification de la personne/porte/ horaires) et sur l'association d'un badge avec une personne, et à la délivrance du badge.

- *La DSI [Direction des Systèmes d'Information] qui est en charge d'assurer le maintien en conditions opérationnelles et en conditions de sécurité du système d'information de l'Administration et d'assurer la gestion des accès physiques. La DSI gère les aspects logiques et techniques des applications utilisées pour l'exploitation du traitement* ».

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 , pour des personnes non affectées à un service ou non autorisées à accéder, aux ressources informatiques du Gouvernement Princier* » et de même, « *de limiter l'accès aux locaux selon des horaires déterminés par les besoins du Service et modulables selon la fonction des personnes concernées* ».

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 :

En ce qui concerne les personnes auxquelles un accès est accordé :

- identité : nom, prénom, matricule ;
- vie professionnelle : service (par association avec les autorisations d'accès de la personne) ;
- informations temporelles ou horodatage : date et heure d'entrée, date et heure de sortie pour l'ensemble des zones ;
- accès aux locaux : identification des zones autorisées ;
- suivi administratif : date de remise du badge, date de restitution, date et motif de déclaration de perte/vol ;
- données d'identification : code d'accès (associé au badge), numéro de badge ou de la Carte d'accès, date de délivrance, date de validité/d'expiration ;
- logs des lecteurs : données d'horodatage, numéro de badge, identification des lecteurs.

En ce qui concerne les gestionnaires de l'application :

- identité : nom, prénom ;
- données d'identification électronique : login, mot de passe ;
- logs de connexion : données d'horodatage, identifiant, actions effectuées.

Les informations relatives à l'identité et à la vie professionnelle des personnes auxquelles un accès est accordé ont pour origine la DRHFFP ou le chef de service.

Les informations temporelles ou horodatage, les accès aux locaux et les logs des lecteurs ont pour origine le système.

Le suivi administratif a pour origine la DRHFFP, les chefs de service et la personne concernée.

Par ailleurs, les informations relatives à l'identité des gestionnaires de l'application ont pour origine la DRHFFP/DSI.

Enfin, les données d'identification électronique et logs de connexion des gestionnaires de l'application ont pour origine le système.

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 Ressources Humaines et de la Formation de la Fonction Publique.

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 « d*e 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 :

- les administrateurs DRHFFP qui déterminent les droits d'accès et les rôles des administrateurs de la DSI de l'application ainsi que les accès des utilisateurs sur les différents obstacles (portes) : lecture/consultation, création, modification/mise à jour et suppression ;
- les administrateurs SPP (Service des Parkings Publics) qui déterminent les accès des utilisateurs sur les différents obstacles (portes) de leur périmètre : lecture/consultation, création, modification/mise à jour et suppression ;
- les administrateurs de la DSI : lecture/consultation, création, modification/mise à jour et suppression ;
- le personnel du prestataire en charge de la maintenance du logiciel et des équipements : lecture/consultation dans le cadre de leurs opérations 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 de quatre rapprochements avec les traitements ayant respectivement pour finalité :

- « *Gestion des dossiers des fonctionnaires et agents de l'Etat relevant de la Fonction Publique et des statuts particuliers* », légalement mis en œuvre ;
- « *Gestion de la messagerie professionnelle Exchange* », légalement mis en œuvre ;
- « Gestion des techniques automatisées de communication (Lotus Notes) », légalement mis en œuvre ;
- « *Assistance aux utilisateurs par le Centre de Service de la DSI* », légalement mis en œuvre.

Le responsable de traitement indique en outre que ledit traitement fait l'objet de deux interconnexions avec les traitements ayant respectivement pour finalité :

- « *Gestion des accès à distance au Système d'Information du Gouvernement* », légalement mis en œuvre ;
- « *Gestion des badges de l'Administration* ».

Ce dernier traitement n'ayant pas fait l'objet de formalité auprès de la CCIN, la Commission demande au responsable de traitement de le lui soumettre dans les plus brefs délais.

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, à la vie professionnelle et les accès aux locaux des personnes auxquelles un accès est accordé ainsi que leurs données d'identification sont conservées tant que la personne travaille au sein de l'Administration + 12 mois après la restitution du badge.

Les informations temporelles ou horodatage sont conservées 12 mois.

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

Les logs des lecteurs concernant les personnes auxquelles un accès est accordé et les logs de connexion des gestionnaires de l'application sont conservés 12 mois glissant.

Enfin l'identité et les données d'identification électronique des gestionnaires de l'application sont conservées tant que la personne exerce cette fonction de gestionnaire.

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 d'un SI.

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

Après en avoir délibéré, la Commission :

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.

Demande que le traitement ayant pour finalité « *Gestion des badges de l'Administration* » lui soit soumis dans les plus brefs délais.

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 par badges aux locaux de l'Administration* ».**

Le Président

Guy MAGNAN