

Délibération n° 2024-019 du 21 février 2024

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

« *Vidéoprotection de l'e-ambassade du Luxembourg* »

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° 2022-331 du 13 juin 2022 portant application de l'article 23 de la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, fixant les mesures de sécurité des systèmes d'information de l'Etat, 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 octobre 2023 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Vidéoprotection de l'e-ambassade du Luxembourg* » ;

Vu la prorogation du délai d'examen de ladite demande d'avis notifiée au responsable de traitement le 21 décembre 2023, 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 21 février 2024 portant examen du traitement automatisé susvisé.

## **La Commission de Contrôle des Informations Nominatives,**

### **Préambule**

L'Administration Gouvernementale souhaite mettre en place un dispositif de vidéoprotection afin d'assurer la sécurité des locaux de l'e-ambassade de Monaco au Luxembourg.

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 « *Vidéoprotection de l'e-ambassade du Luxembourg* ».

Les personnes concernées sont « *toutes les personnes accédant aux zones sous vidéosurveillance* », les opérateurs vidéo pour l'e-ambassade et les administrateurs du système de vidéoprotection.

Enfin, les fonctionnalités sont les suivantes :

- assurer la sécurité des personnes ;
- assurer la sécurité des biens ;
- guider les personnes habilitées à avoir accès à la zone lors des interventions ;
- surveiller l'exécution des actions réalisées par les personnes habilitées à avoir accès à la zone ;
- vérifier les zones lors du déclenchement d'alerte (ex. porte restée ouverte) ;
- constater l'intrusion et constituer des preuves en cas d'infractions.

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.

L'intérêt légitime mis en avant est celui d'« *assurer la protection des personnes, des biens et des ressources informatiques dont il a la charge* ».

La Commission prend ainsi note que la « *la mise en place d'un système de vidéosurveillance participe à la sécurité des locaux à des fins préventives et correctives en cas d'effraction ou de négligence* » ainsi qu'à « *la sécurité physique des personnes intervenant sur un site distant* » puisque « *les intervenants peuvent être seuls sur les lieux. Les agents de sécurité du Data center ne sont pas habilités à entrer dans les zones. Il importe donc que la personne puisse être suivie à*

*distance et qu'une alerte puisse être lancée en cas de malaise ou d'accident impactant la personne ».*

Le responsable de traitement précise par ailleurs que le traitement s'inscrit notamment dans le cadre de l'application de mesures physiques demandées par la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE), annexée à l'Arrêté Ministériel n° 2022-331 du 13 juin 202.

La Commission constate ainsi que le traitement dont s'agit répond, notamment, aux objectifs inhérents à l'exploitation des systèmes d'information et à ceux portant sur les contrôles, particulièrement :

- *« Axe 3.5 : Sécurité physique des locaux abritant les systèmes d'information : Inscire la sécurisation physique des systèmes d'information dans la sécurisation physique des locaux et dans les processus associés.*
- *Axe 3.6 : 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.*
- *Axe 4.7 : 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 ».*

Elle relève que le dispositif dont s'agit *« participe également aux mesures techniques mises en place pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, attendues par l'article 17 de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives ».*

A cet égard, le responsable de traitement indique que *« La gestion des accès repose, notamment, sur la mise en place de système de vidéosurveillance permettant :*

- *de protéger l'accès à l'e-ambassade tenant compte de la sensibilité des locaux, des équipements y hébergés ou des activités y exécutées, de la localisation des locaux ;*
- *de s'assurer en réel que la personne qui entre dans la zone est bien la personne attendue ;*
- *de mettre en place la procédure dite « Hands and eyes » sous surveillance de la DSI, soit une délégation d'actions réalisées à distance, ou d'accompagner les agents de la DSI lorsque les actions sont réalisées par eux afin de guider si nécessaire l'opérateur, de s'assurer que la personne intervient sur la zone et/ou sur les équipements définis, que des équipements ne sont pas déplacés ou ôtés alors qu'ils ne devraient pas...*
- *de veiller à la sécurité physique de ces personnes qui pourraient être seules dans le data center, en complément du système dit d'homme mort. En effet, [la société de sécurité] n'a pas le droit d'entrer dans les salles de l'e-ambassade. Dans le coffre du local technique de l'e-ambassade, accessible par [la société de sécurité] en cas d'incident, est déposé une carte d'accès en cas d'urgence. Le code de ce coffre est alors communiqué au gardien pour lui permettre d'entrer dans la salle et d'aider la personne en difficulté ».*

La Commission prend acte qu'*« Aucune personne ne travaille de manière permanente dans les salles du data center »* mais que *« Des personnes peuvent y réaliser ponctuellement des actions programmées sur instruction de la DSI ».*

Elle relève également que *« L'implantation des caméras a été réfléchi en tenant compte des couloirs, des zones d'accès et de circulation, mais aussi d'aspects fonctionnels, comme la possibilité de visualiser l'intérieur des baies lorsque les portes sont ouvertes, selon que les portes*

sont pleines, en quart ou en demi pour permettre de visualiser les actions effectuées dans les baies ».

Enfin, la Commission relève que les caméras ne sont pas mobiles et que les fonctionnalités zoom et micro ne sont pas activées.

Au vu de ce qui précède, elle 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 : image, silhouette, visage ;
- données d'identification électronique : login, mot de passe des personnes habilitées à avoir accès aux images ;
- informations temporelles : numéro de la caméra, emplacement des caméras, date et heure de la prise de vue ;
- logs de connexion des personnes habilitées.

Les informations ont pour origine le système de vidéoprotection, à l'exception du login qui a pour origine la DSI et du mot de passe qui a pour origine la personne concernée.

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'un affichage.

A l'analyse de ce document, la Commission constate que celui-ci ne mentionne pas la possibilité pour toute personne concernée d'exercer son droit d'accès par voie électronique.

Elle demande donc que l'affichage soit complété afin d'indiquer que le droit d'accès s'exerce par voie postale ou par courrier électronique.

La Commission rappelle par ailleurs que cet affichage doit garantir une information visible, lisible et claire de la personne concernée et être apposé à chaque entrée de l'établissement.

Sous ces conditions, elle considère que les modalités d'information préalable des personnes sont conformes aux dispositions de 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 responsable de traitement indique que le droit d'accès s'exerce par voie postale ou par courrier électronique auprès de la Délégation Interministérielle chargée de la Transition Numérique (DITN).

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

Elle précise que la réponse à une demande de droit d'accès pourra s'effectuer sur place, auprès de la DITN, mais également au sein des locaux de l'e-ambassade.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, elle constate qu'une procédure a été mise en place pour permettre au responsable de traitement de s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

La Commission considère ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

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

### **➤ *Sur les destinataires***

Les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique.

La Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

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 :

- l'opérateur des accès de l'e-ambassade : consultation au fil de l'eau ;
- le personnel habilité de la DSI : tous droits dans le cadre de ses opérations de maintenance ;
- la direction de la DSI via une demande auprès du personnel habilité de la DSI : consultation au fil de l'eau et en différé, extraction
- le prestataire technique à la demande de la DSI : tous droits, à l'exception de l'extraction, dans le cadre de la maintenance.

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

La Commission constate par ailleurs que les accès distants (PC) utilisés sur le réseau de vidéosurveillance par la DSI et le prestataire sont sécurisés.

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'un rapprochement avec un traitement ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DSI* ».

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

- « *Gestion de la messagerie professionnelle* » ;
- « *Gestion des accès dédiés au Système d'information du Gouvernement* » ;
- « *Gestion et analyse des évènements du système d'information* » ;
- « *Gestion des accès par badges aux sites spécifiques de l'Administration* ».

La Commission prend acte que ces traitements ont été légalement mis en œuvre.

## **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 constate par ailleurs que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

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 informations sont conservées 1 mois, à l'exception des identifiants et mots de passe qui sont conservés tant que la personne est en place.

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

### **Après en avoir délibéré, la Commission :**

#### **Constata que :**

- les accès distants (PC) utilisés sur le réseau de vidéosurveillance par la DSI et le prestataire sont sécurisés ;
- la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

#### **Rappelle que :**

- l'affichage doit garantir une information visible, lisible et claire de la personne concernée et être apposé à chaque entrée de l'établissement ;
- les Services de Police monégasque ne pourront avoir communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- 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.

**Précise que** la réponse à une demande de droit d'accès pourra s'effectuer sur place, auprès de la DITN, mais également au sein des locaux de la e-ambassade.

**Demande que** l'affichage soit complété afin d'indiquer que le droit d'accès s'exerce par voie postale ou par courrier électronique.

**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 « *Vidéoprotection de l'e-ambassade du Luxembourg* ».**

Le Président

Guy MAGNAN