Délibération n° 2019-137 du 18 septembre 2019

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

« *Sécurisation des accès à distance au SI pour les flottes nomades BYOD et professionnelles*»,

Dénommé « *Mobile Iron* »

exploité par la Direction des Réseaux et 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 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 7 juin 2019, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Sécurisation des accès à distance au SI pour les flottes nomades BYOD et professionnelles* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 5 aout 2019, 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 18 septembre 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

L'Administration permet aux fonctionnaires et agents de l'Etat, ainsi qu'aux prestataires de ce dernier qui le demandent, de déployer sur leurs terminaux (smartphone, mobile) personnels ou professionnels l'application Mobile Iron « *afin de permettre l'accès à distance sécurisé à des contenus identifiés localisés sur le SI du Gouvernement. Ces contenus pourront être du mail, des applications Web, et toute application paramétrée pour être accessible par Mobile Iron au fur et à mesure des développements des métiers du Gouvernement et des besoins exprimés* ». Ces demandes sont effectuées par l'ouverture de tickets soumises à l'approbation des chefs de service des personnes concernées.

Il s'agit ainsi de créer sur les terminaux des fonctionnaires, agents et prestataires qui en ont le besoin un conteneur permettant de sécuriser l'accès aux applications autorisées par l'Administration. Il est en effet précisé que « *seules les applications ciblées comme pouvant être mises à disposition des agents peuvent être installées dans le conteneur* ».

La mise en place de cette solution nécessite ainsi la collecte et l'exploitation d'informations nominatives. Aussi, le traitement d'informations nominatives y afférent 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 « *Sécurisation des accès à distance au SI pour les flottes nomades BYOD et professionnelles* ».

Il est dénommé « *Mobile Iron* ».

Il concerne les fonctionnaires et agents de l'Etat, ainsi que les prestataires, qui souhaitent disposer de l'application.

Les fonctionnalités du traitement sont :

- Création d'un compte Mobile Iron pour mettre en place les connectivités ;
- Enrôlement des terminaux dans l'interface administration Mobile Iron ;
- Authentification des utilisateurs pour un accès à distance sécurisé ;
- Support utilisateurs à distance ;
- Gestion des licences Mobile Iron dans une Interface Homme Machine (IHM) de management Mobile Iron ;
- Suivi des formations des agents de la DRSI à l'exploitation et la maintenance applicative ;
- Etablissement de statistiques et tableaux de bord.

La Commission constate 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 et la réalisation d'un intérêt légitime, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission relève que la mise en place d'un tel outil résulte des attributions conférées à la DRSI, qui doit assurer la disponibilité des ressources informatiques en environnement sécurisé, conformément aux dispositions de l'Ordonnance n° 7.012 du 20 juillet 2018 qui porte création ce celle-ci. A cet égard, il est spécifié que « *le traitement est justifié par une nécessité de sécurisation des accès au SI du Gouvernement au moyen d'appareils mobiles* ».

Il est en outre précisé, en ce qui concerne la justification par une obligation légale, que le traitement doit être conforme 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. S'il ne s'agit pas directement d'une obligation légale imposant la mise en œuvre du présent traitement, la prise en compte de manière obligatoire de la PSSIE dans son exploitation participe nécessairement à sa sécurité. La PSSIE impose notamment des obligations procédurales dans la gestion et la révocation de droits d'accès aux systèmes d'information, la gestion des privilèges, etc.

De plus, il est fait référence à la Charte des systèmes d'information de l'Etat annexée à l'Arrêté Ministériel n° 2015-703 du 26 novembre 2015, et à la Charte « *Administrateur réseaux et système d'information de l'Etat* », qui imposent aux utilisateurs et admirateurs des systèmes d'Information de l'Etat des obligations propres à leurs fonctions.

Le responsable de traitement explique également qu'un « *procès-verbal de mise à disposition de l'application Iron Mobile est signé par l'utilisateur avant l'enrôlement. Les mentions obligatoires de l'article 14 de la Loi n° 1.165 y ont été intégrées* ».

Enfin, la Commission relève de l'analyse du dossier que si « *l'administrateur pourra avoir accès aux éléments installés dans le conteneur* », « *il saura ce qui est installé comme applications mais en aucun cas ne pourra avoir accès au contenu* », étant encore précisé que « *l'administrateur n'a pas accès aux éléments qui ne sont pas installés dans le conteneur* ».

La Commission en prend acte et 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 utilisateurs :

- identité : nom, prénom ;
- coordonnées professionnelles : email professionnel, pays, numéro de téléphone mobile ;
- informations temporelles : adresse mac, adresse IP, log de connexion, date de la dernière connexion, durée de connexion totale ;
- identification du téléphone : type de téléphone, marque de téléphone, numéro IMEI, opérateur ;

- éléments administratifs de suivi : date d'enregistrement, numéro de licence, date d'initialisation, date de fin, statut (active).

En ce qui concerne les agents de la DRSI intervenant sur les consoles :

- identité du signataire : nom, prénom ;
- coordonnées professionnelles : email, numéro de téléphone ;
- vie professionnelle : fonction, rôle sur l'application, date de formation ;
- données de connexion : log de connexion.

En ce qui concerne les rédacteurs de documentation :

- identité : nom, prénom ;
- vie professionnelle : rôle ;
- horodatage : date et heure de création puis de mise à jour des documents.

Les informations relatives à l'identité de l'utilisateur, son email et son pays ont pour origine le traitement relatif à la gestion des habilitations (Active Directory).

Le numéro de téléphone mobile et les données d'identification du téléphone sont fournis par la personne concernée.

En outre, la DRSI effectue l'inscription des éléments administratifs de suivi.

Les informations relatives au rédacteur sont produites par ce dernier.

De plus, l'inscription de l'identité et la vie professionnelle des agents de la DRSI est choisie par la Direction.

Les informations temporelles sont collectées par Syslog, tandis que les données de connexion sont produites par le système.

Les coordonnées professionnelles des agents de la DRSI ont pour origine les traitements relatifs aux messageries de l'Administration.

Toutefois, la Commission constate à l'analyse du dossier que les informations relatives à la génération d'une demande (personne effectuant la demande/personne concernée) ont pour origine le traitement d'assistance aux utilisateurs, qui est le canal conduisant à la création d'un profil.

De plus, la Commission relève que le traitement relatif à la gestion des habilitations ne contient pas d'information relative au pays des personnes concernées.

Aussi, en l'absence de justification quant à la nécessité de cette information et compte tenu des incertitudes sur son origine, la Commission demande à ce qu'elle ne soit pas collectée. Une justification ultérieure pourra être portée à la connaissance de la Commission.

Elle relève également des pièces communiquées que des données de roaming des utilisateurs de la solution sont accessibles à ses administrateurs dès lors qu'il ne s'agit pas du réseau Monaco Telecom.

Si la Commission peut considérer proportionné que le responsable de traitement sache si l'utilisateur est présent ou non sur le territoire monégasque, elle estime que toute information plus précise relative à la localisation (France, Italie, etc.) est disproportionnée, et en exclut donc la collecte.

Enfin, la Commission relève que Syslog collecte les adresses IPs utilisées par les personnes concernées, qui peuvent être celles de tiers qui sont en relation avec elles. Aussi, en l'absence de justification en lien avec des questions de sécurité, la Commission exclut la collecte des adresses IPs.

Sous ces réserves, 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 est réalisée par le biais d'un procès-verbal de mise à disposition de Mobile Iron.

Toutefois ce document n'est pas joint à la demande d'avis.

Aussi la Commission rappelle que l'information des personnes concernées doit être effectuée conformément à l'article 14 de la Loi n° 1.165.

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

Le droit d'accès est exercé par voie postale ou sur place auprès de la Direction des Réseaux et 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

La Commission constate que les informations objets du traitement sont susceptibles d'être communiquées aux autorités compétentes en cas de litige.

Les accès sont définis comme suit :

- Administrateurs Mobile Iron du Centre de Service (5 personnes) : tout accès, notamment pour l'enrôlement des terminaux, la création de compte ;

- Administrateurs de l'infrastructure (5 personnes) : accès aux logs de connexion à partir de la console Management Mobile Iron ;

- Prestataire (intégrateur) : accès à des fins d'administration des systèmes.

La Commission constate ainsi qu'il est fait recours à un 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 de ce dernier 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.

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 rapproché avec le traitement ayant pour finalité « *Gestion des habilitations et des accès au système d'information par l'Active Directory* » légalement mis en œuvre, pour identifier le demandeur et effectuer l'enrôlement, et est interconnecté avec les traitements suivants :

- Gestion des techniques automatisées de communication, légalement mis en œuvre, pour permettre l'échange de messages entre intervenants ;
- Assistance aux utilisateurs par le Centre de Service de la DRSI, non légalement mis en œuvre, « *pour le process de demande d'enrôlement et la validation des opérations subséquentes, puis des demandes qui pourraient être effectuées par les utilisateurs comme pour toute utilisation du SI* » ;
- Gestion de la messagerie professionnelle (exchange), en cours d'analyse, pour permettre l'échange de messages entre intervenants ;
- Gestion des accès à distance du Système d'Information du Gouvernement, concomitamment analysé, pour permettre au prestataire d'effectuer les opérations relevant de sa compétence.

Il est enfin précisé que le présent traitement sera interconnecté avec tous les futurs traitements qui seront accessibles par Mobile Iron.

Concernant le traitement ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DRSI* », la Commission demande à ce qu'il lui soit soumis dans les meilleurs 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.

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 jusqu'à la suppression de l'application à la suite du départ de l'intéressé ou à sa demande en ce qui concerne les données d'identité, de coordonnées, d'identification du téléphone et aux éléments administratifs de suivi de l'utilisateur.

Les données des agents de la DRSI relatives à leur identité, coordonnées professionnelles et vie professionnelle sont conservées tant que la personne travaille sur le projet.

Les informations en lien avec les rédacteurs de documentation sont accessibles tant que le document est utile dans la base.

Enfin, les informations temporelles et les données de connexions sont supprimées tous les 4 mois glissants.

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

Après en avoir délibéré, la Commission :

Constate que les informations relatives à la génération d'une demande (personne effectuant la demande/personne concernée) ont pour origine le traitement d'assistance aux utilisateurs.

Rappelle que :

- l'information des personnes concernées doit être effectuée en conformité avec l'article 14 de la Loi n° 1.165 ;

- 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.

Demande que :

- le traitement ayant pour finalité « *assistance aux utilisateurs par le Centre de Service de la DRSI* » lui soit soumis dans les meilleurs délais;

- les données de roamings, si elles précisent la localisation hors Monaco, soient exclues du présent traitement ;

- les adresses IPs utilisées par les personnes concernées ne soient pas collectées ;

- l'information du pays de la personne concernée ne soit pas collectée, en l'absence de justification sur sa nécessité et les incertitudes sur l'origine de sa collecte.

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 *« Sécurisation des accès à distance au SI pour les flottes nomades BYOD et professionnelles ».***

Le Président

Guy MAGNAN