Délibération n° 2018-090 du 20 juin 2018

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Contrôle des accès aux locaux de la banque par badge non biométrique* »

présenté par la Compagnie Monégasque de Banque

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° 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° 2010-43 du 15 novembre 2010 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail mis en œuvre par les personnes physiques ou morales de droit privé ;

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'autorisation déposée par la Compagnie Monégasque de Banque (CMB) le 19 avril 2018 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Contrôle des accès sur le lieu de travail par badge non biométrique* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 18 juin 2018, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 20 juin 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Compagnie Monégasque de Banque (CMB) est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 76S1557, ayant pour activité « *de faire, en tous pays, toutes opérations de banque, de finance, de crédit, d'escompte, de commission, de bourse et de change, pour elle-même, pour le compte de tiers ou en participation et d'une façon générale, sous les seules restrictions résultant des dispositions légales en vigueur, toutes opérations pouvant se rattacher à l'objet social* ».

Afin d'assurer la sécurité des biens et des personnes au sein de ses locaux, cette société souhaite installer un système de contrôle des accès par badges magnétiques.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance, il relève donc du régime de l'autorisation préalable visé à l'article 11-1 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 « *Contrôle des accès sur le lieu de travail par badge non biométrique ».*

Les personnes concernées sont les employés de banque ainsi que les prestataires de services.

Enfin, les fonctionnalités sont les suivantes :

- contrôler l'accès aux entrées et sorties de la banque ;
- contrôler l'accès à certains locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- contrôler l'accès des visiteurs (prestataires de services) ;
- gérer les habilitations d'accès aux personnes autorisées ;
- désactiver les badges perdus ou volés ;
- permettre, le cas échéant, la constitution de preuves en cas d'infraction.

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 de contrôle concerne les accès aux locaux de la banque et s'effectue par le biais d'un badge non biométrique.

Par conséquent, elle modifie la finalité comme suit : « *Contrôle des accès aux locaux de la banque par badge non biométrique* ».

II. Sur la licéité et la justification du traitement

Le traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable du traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission constate ainsi que dans le cadre de ses activités, « *la Compagnie Monégasque de Banque est amenée à détenir et à exploiter des données pour le compte de ses clients, et notamment des données relatives à ses activités bancaires* » et que ce système de contrôle d'accès par badge lui « *permet d'assurer la protection des personnes et des biens* » ainsi que « *la confidentialité des données détenues grâce à une restriction d'accès aux locaux aux seules personnes dûment habilitées* ».

Elle relève par ailleurs que les personnes concernées « *bénéficient d'une information préalable et suffisante* » sur l'existence et l'exploitation du traitement.

Enfin, la Commission note que ledit traitement n'a pas pour objet de « *contrôler de manière inopportune les comportements, les habitudes et les horaires des personnes concernées* par le traitement ».

Au vu de ce qui précède, elle considère que le 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

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité: nom, prénom, numéro de badge interne, service ;
- formation-diplômes/Vie professionnelle : service, fonction, plages horaires habituellement autorisées, zones d'accès autorisées, durée de l'autorisation ;
- informations temporelles : date et heure d'entrée et de sortie, de passage à une zone à accès restreint ;
- accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie, ou point de passage ;
- prestataires de services : nom, prénom, dates et heures de visite, société d'appartenance ;
- badge ou carte : numéro de badge ou de la carte, date de délivrance, date de validité, état (activé ou désactivé).

La Commission constate par ailleurs que les logs de connexion des personnes habilitées à avoir accès aux informations sont également collectés et que ceux-ci ont pour origine le système de badges.

Les informations relatives à l'identité des personnes ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* ».

Les informations relatives à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* » ainsi que le Service CPRM (Controle Permanent et Risk Management) en ce qui concerne la détermination des zones d'accès autorisées.

Les informations relatives aux informations temporelles et aux badges ont pour origine le système de badges.

Enfin, les informations relatives aux prestataires de services ont pour origine lesdits prestataires de services.

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***

Le responsable de traitement indique que l'information préalable s'effectue par le biais d'un document spécifique.

A l'analyse de ce document, la Commission 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 droit d'accès s'exerce par courrier électronique.

A cet égard, la Commission considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement 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 condition, la Commission constate 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 aux Autorités policières et judiciaires légalement habilitées.

La Commission estime que ces communications peuvent être justifiées pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, les Autorités policières et judiciaires pourront avoir communication des informations que dans le strict cadre de leurs missions légalement conférées.

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

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

Le responsable de traitement indique que « *Le chef de service ainsi que le chef de service adjoint du département « Services Généraux » disposent des droits d'inscription, de modification, et de consultation afférents aux informations collectées dans le cadre du traitement dont s'agit. En ce qui concerne les données relatives aux zones d'accès autorisées, elles sont disponibles en inscription, modification, et consultation par le Département CPRM ou Contrôle Périodique et Risk*

Management. Elles sont également disponibles en consultation uniquement par les Services Généraux afin que ces derniers puissent programmer les badges d'accès en conséquence ».

Il indique également que « *Les deux prestataires externes pouvant intervenir sur le système pour leurs tâches de maintenance interviennent sur site uniquement* ».

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 les prestataires de services, 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 leur contrat de prestation de service. De plus, lesdits prestataires de services sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

La Commission rappelle enfin qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

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 « *Gestion administrative des salariés* » ; traitement 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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Elle 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.

Enfin, la Commission rappelle que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations relatives à l'identité, à la formation, aux diplômes, à la vie professionnelle sont conservées 5 ans après le départ de l'employé de la banque.

Les informations temporelles, les informations relatives aux accès aux locaux et les informations relatives aux badges sont conservées 3 mois.

Enfin, les informations relatives aux prestataires de services sont conservées 3 mois à compter du départ du salarié pour les prestataires de services ou 3 mois à compter de la visite pour les autres prestataires de services.

Par ailleurs, la Commission fixe la durée de conservation des logs de connexion à un an maximum.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion des accès aux locaux de la banque par badge non biométrique* ».

Constate que les logs de connexion des personnes habilitées à avoir accès au traitement sont également collectés.

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que :

- les Autorités policières et judiciaires ne pourront avoir communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;

- 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 ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Fixe la durée de conservation des logs de connexion à un an maximum.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par la Compagnie Monégasque de Banque du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle des accès aux locaux de la banque par badge non biométrique*».**

Le Président

Guy MAGNAN