

Délibération n° 2017-111 du 21 juin 2017

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

« *Sécurité et contrôle d'accès aux locaux par badge biométrique reposant sur la reconnaissance de l'empreinte digitale* »

présenté par Martin Maurel Sella Banque Privée – Monaco S.A.M.

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° 2011-33 du 11 avril 2011 portant recommandation sur la reconnaissance de l'empreinte digitale, exclusivement enregistrée sur un support individuel détenu par la personne concernée, ayant pour finalité le contrôle d'accès à des zones limitativement identifiées sur le lieu de travail, mis en œuvre par une personne physique ou morale de droit privé ;

Vu la demande d'autorisation déposée par Martin Maurel Sella Banque Privée – Monaco S.A.M. le 11 avril 2017 concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Sécurité et contrôle d'accès aux locaux par badge biométrique* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 8 juin 2017, conformément à l'article 11.1 de la Loi n°1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 21 juin 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Martin Maurel Sella Banque Privée – Monaco S.A.M., est une société immatriculée au RCI sous le n° 00S03802, ayant notamment pour activité « [...] la réalisation de toutes opérations de banque ou connexes telles que définies par la « loi bancaire » applicable (...) ».

Afin de restreindre l'accès à ses locaux aux seules personnes habilitées, elle souhaite mettre en place un système biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance et comporte des données biométriques nécessaires au contrôle de l'identité des personnes, 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 traitement a pour finalité « Sécurité et contrôle d'accès aux locaux par badge biométrique ».

Les personnes concernées sont les employés.

Enfin, les fonctionnalités du traitement sont :

- la sécurité des personnes et des biens en contrôlant les accès à des zones restreintes des locaux (notamment le SAS d'entrée de la banque), et ce à l'aide d'un lecteur de contrôle d'accès biométrique ;
- la gestion de la création des badges (procédure d'enrôlement) ;
- la gestion des habilitations d'accès aux personnes autorisées ;
- la désactivation des badges perdus/volés ;
- 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 ce système de badge biométrique repose sur la reconnaissance de l'empreinte digitale.

Par conséquent, elle modifie la finalité comme suit : « Sécurité et contrôle d'accès aux locaux par badge biométrique reposant sur la reconnaissance de l'empreinte digitale ».

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.

A cet égard, le responsable de traitement précise que ce dispositif va permettre d'« assurer la protection des personnes et des biens » mais aussi « d'assurer la confidentialité des données détenues grâce à une restriction d'accès aux locaux aux seules personnes dûment habilitées ».

La Commission note par ailleurs que ledit dispositif « n'a pas pour objet de contrôler de manière inopportune le comportement, les habitudes et les horaires des personnes concernées par le traitement » et qu'il ne permet pas la reconnaissance de l'empreinte digitale avec stockage dans une base de données centralisée ou sur un terminal de lecture-comparaison.

Elle relève également que les empreintes sont stockées dans un badge détenu par l'enrôlé et qu'aucune empreinte n'est stockée dans le capteur biométrique ou dans le serveur, conformément à sa délibération n° 2011-33 du 11 avril 2011 portant recommandation sur les dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale.

Elle souligne de plus que, au regard de la nature de l'établissement, la mise en place d'un tel dispositif est justifiée.

Au vu de ce qui précède, la Commission considère donc 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 traitées

Les informations exploitées aux fins du présent traitement sont :

- identité : nom, prénom ;
- formation – diplômes – vie professionnelle : famille d'accès, plage horaire spécifique ;
- données d'identification électronique : logs de connexion des personnels habilités à avoir accès aux informations et au traitement ;
- données biométriques : gabarit de l'empreinte digitale ;
- horodatage des accès aux locaux : date et heure d'entrée, nom et/ou numéro de la zone/porte d'entrée ;
- badge : numéro de badge, date de délivrance, état (activé ou désactivé).

Les informations relatives à l'identité, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative du personnel* ».

Les informations relatives aux données d'identification électronique, à l'horodatage des accès aux locaux et au badge ont pour origine le système biométrique.

Les informations relatives aux données biométriques, à savoir le gabarit de l'empreinte digitale, ont pour origine l'employé.

Au vu de ce qui précède, la Commission considère que les informations traitées 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 des personnes concernées

Le responsable de traitement indique que l'information préalable est effectuée au moyen d'une mention ou clause particulière intégrée dans un document remis à l'intéressé.

Les documents joints au dossier ne lui permettant pas de déterminer que l'information de l'ensemble des personnes concernées est assurée, la Commission rappelle que cette information doit impérativement être effectuée conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

➤ Sur l'exercice du droit d'accès des personnes concernées

Le droit d'accès s'exerce par voie postale ou sur place auprès du Responsable de la Conformité et du Contrôle Interne.

La réponse à ce droit d'accès s'exerce selon les mêmes modalités.

Le délai de réponse est de 30 jours.

La Commission considère 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

Le responsable de traitement indique que des informations sont susceptibles d'être communiquées aux Autorités policières et judiciaires légalement habilitées.

La Commission estime ainsi que la communication aux Autorités policières et judiciaires peut être justifiée par les besoins d'une enquête. A cet égard, elle rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

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

➤ Sur les personnes ayant accès au traitement

Les personnes ayant accès au traitement sont :

- le Directeur Administratif et son adjoint : accès en inscription, modification, mise à jour et consultation ;
- le Responsable Ressources Humaines : accès en inscription, modification, mise à jour et consultation ;
- le personnel habilité du prestataire en charge de l'assistance et de la maintenance : accès en inscription, modification, mise à jour et consultation, sous la supervision du personnel de la Banque habilité.

S'agissant de l'accès aux informations par le service des Ressources Humaines, la Commission considère que cet accès ne pourra être justifié que dans le cadre des fonctionnalités prévues par ledit traitement et exclut donc expressément toute autre utilisation qui pourrait en être faite à des fins disciplinaires sortant du cadre de la sécurité des personnes et des biens.

Sous cette condition, elle considère que les accès susvisés sont justifiés.

En ce qui concerne le prestataire, la Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, ses droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, celui-ci est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Elle constate 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 est tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

VI. Sur les interconnexions

Le responsable de traitement indique que le présent traitement fait l'objet d'un rapprochement avec un traitement ayant pour finalité « *Gestion Administrative du personnel* », 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.

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

Elle 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

La Commission constate que les informations relatives à l'identité, à la formation, aux diplômes, à la vie professionnelle et au badge sont conservées 5 ans après la fin du contrat de travail, que les données d'identification électronique sont conservées 3 mois après la connexion, que les données biométriques sont conservées pendant la durée de l'habilitation de l'employé à pénétrer les zones faisant l'objet d'une restriction et l'horodatage des accès aux locaux est conservé 1 mois après le passage dans la zone/porte considérée.

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

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Sécurité et contrôle d'accès aux locaux par badge biométrique reposant sur la reconnaissance de l'empreinte digitale* ».

Constata que la liste nominative des personnes ayant accès au traitement est tenue à jour et précise qu'elle doit lui être communiquée à première réquisition.

Considère que l'accès au traitement par le service des Ressources Humaines ne peut être justifié que dans le cadre des fonctionnalités prévues par le présent traitement.

Exclut l'utilisation des données faite à des fins sortant du cadre de l'atteinte aux biens et aux personnes.

Rappelle que :

- l'information préalable des personnes concernées doit être effectuée conformément à l'article 14 de la Loi n° 1.165 ;
- les Autorités judiciaires et policières ne peuvent 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) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

A la condition de la prise en compte des éléments qui précèdent,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par Martin Maurel Sella Banque Privée – Monaco S.A.M. du traitement automatisé d'informations nominatives ayant pour finalité « Sécurité et contrôle d'accès aux locaux par badge biométrique reposant sur la reconnaissance de l'empreinte digitale ».**

Le Président

Guy MAGNAN