

Délibération n° 2019-051 du 20 mars 2019

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

« *Gestion du système de vidéosurveillance des locaux* »

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 la Loi n° 1.264 du 23 décembre 2002 relative aux activités privées de protection des personnes et des biens ;

Vu l'Ordonnance Souveraine n° 15.699 du 26 février 2003 fixant les conditions d'application de la Loi n° 1.264 du 23 décembre 2002 susvisée ;

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° 2010-13 du 3 mai 2010 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs de vidéosurveillance 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 l'autorisation délivrée par le Ministre d'Etat en date du 26 novembre 2018 ;

Vu la demande d'autorisation déposée par la Compagnie Monégasque de Banque le 4 décembre 2018 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion du système de vidéosurveillance des locaux* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 1<sup>er</sup> février 2019, 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 mars 2019 portant examen du traitement automatisé susvisé.

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

### **Préambule**

La Compagnie Monégasque de Banque est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 76S01557 , ayant pour objet « *de faire dans la Principauté de Monaco et à l'étranger, pour son compte, pour le compte de tiers ou en participation, toutes opérations bancaires et financières et plus généralement toutes opérations pouvant être exercées par les établissements de crédit de droit monégasque en conformité avec la législation et la réglementation qui leur sont applicables et notamment les activités de courtage y compris de produits d'assurance. Effectuer toutes opérations commerciales ou financières, mobilières ou immobilières pouvant se rattacher à l'objet social ou à tous objets similaires ou connexes. Le Conseil d'Administration aura la faculté de créer des filiales, succursales, bureaux de représentation en tous pays, sans qu'il puisse en résulter une dérogation aux règles de compétence édictées par les présents statuts* ».

Afin d'assurer la sécurité des biens et des personnes au sein des locaux de la Compagnie Monégasque de Banque, situés 23 Avenue de la Costa, cette société souhaite installer un système de vidéosurveillance.

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**

Ce traitement a pour finalité « *Gestion du système de vidéosurveillance des locaux* ».

Les personnes concernées sont : les employés de la banque, ainsi que toute personne amenée à pénétrer dans les locaux de l'établissement.

Enfin, les fonctionnalités sont les suivantes :

- assurer la sécurité des personnes ;
- assurer la sécurité des biens ;
- permettre la constitution de 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**

### **➤ Sur la licéité**

Dans le cadre de sa recommandation n° 2010-13 du 3 mai 2010, la Commission rappelle les conditions de licéité d'un traitement de vidéosurveillance, au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

A ce titre, elle estime que la licéité d'un tel traitement est attestée par l'obtention de l'autorisation du Ministre d'Etat, conformément aux dispositions des articles 5 et 6 de la Loi n° 1.264 du 23 décembre 2002.

En l'espèce, cette pièce délivrée le 26 novembre 2018 est jointe au dossier de demande d'autorisation.

La Commission considère donc que le traitement est licite conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

### **➤ Sur la justification**

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, la Commission constate que *« la mise en œuvre du traitement permet la réalisation d'un intérêt légitime qui est celui de la protection des personnes et des biens, sans méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée, laquelle bénéficie d'une information quant à la mise en place du traitement. La sécurité des biens et des personnes constitue un objectif essentiel, lequel objectif justifie que ce traitement soit mis en œuvre à des fins de surveillance »*.

Elle constate également par le biais des captures d'écrans fournies par le responsable de traitement qu'une caméra est placée au-dessus du distributeur automatique de billets (DAB) de l'agence Costa.

La Commission rappelle toutefois qu'aucun code secret renseigné sur ledit distributeur automatique de billets par le client ne devra être visualisé.

Elle note également que le dispositif de vidéosurveillance *« ne permet pas de contrôler le travail ou le temps de travail d'un salarié »*.

Le responsable de traitement précise par ailleurs que le présent traitement *« ne conduit pas à un contrôle permanent et inopportun des personnes concernées »*.

La Commission note par ailleurs que parmi l'ensemble des caméras installées au sein du dispositif, quatre sont *« de simples « fenêtres » qui n'enregistrent pas les images. Ces « fenêtres » servent uniquement aux caissiers afin que les différentes caisses ne soient pas engorgées par les clients lors de leur venue dans nos locaux, et ce dans un souci de sécurité et de confidentialité vis-à-vis de notre clientèle »*.

Enfin, elle relève que les caméras ne sont pas mobiles et que la fonctionnalité micro n'est pas activée. En revanche, les caméras sont dotées de la fonction zoom.

### **III. Sur les informations nominatives traitées**

Les informations nominatives traitées sont :

- Identité : image, visage et silhouette des personnes ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux images ;
- informations temporelles et horodatage : lieu et identification des caméras, date et heure de la prise de vue.

Ces informations ont pour origine le système de vidéosurveillance.

La Commission considère donc 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, ainsi que par une procédure interne accessible en Intranet.

L'affichage n'ayant pas été joint à la demande d'autorisation, la Commission rappelle qu'en application de sa recommandation n° 2010-13 du 3 mai 2010, ledit affichage doit comporter, *a minima*, un pictogramme représentant une caméra, ainsi que le nom du service auprès duquel s'exerce le droit d'accès en Principauté.

Elle rappelle par ailleurs que cet affichage doit, conformément à sa recommandation n° 2010-13 du 3 mai 2010, garantir une information visible, lisible et claire de la personne concernée et être apposé à chaque entrée de l'établissement.

Sous ces conditions, 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 voie postale et courrier électronique. La réponse à ce droit d'accès s'exerce sur place.

Le délai de réponse à une demande de droit d'accès est de 30 jours.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, 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.

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 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**

Le responsable de traitement indique que « *Le recours à la lecture directe d'images sur les équipements est effectué par les Services Généraux, qui peuvent consulter ou extraire les données, sur accord du Responsable du Contrôle Périodique saisi de la demande d'accès.*

*Ce recours doit se faire à minima selon le processus « 4 yeux », c'est-à-dire en la présence de l'une des personnes suivantes :*

- *le Responsable de la Conformité ou le Responsable Juridique uniquement dans les cas suivants :*
  - *Toute recherche ou constitution de preuves en cas de litige ou de poursuite ;*
  - *Toute requête des services de Police.*
- *le DRH pour tout visionnement intéressant un salarié ;*
- *le RSSI uniquement en cas d'interventions techniques sur les équipements Hardware et Software. »*

Le responsable de traitement précise également que « *Le prestataire technique externe peut se déplacer sur demande des collaborateurs des Services Généraux pour effectuer des opérations de maintenance. Dans ce cas, cela se fera toujours en présence des collaborateurs du Département des Service Généraux.* »

Concernant la Direction des Ressources Humaines, la Commission rappelle qu'un tel accès en consultation ne peut s'effectuer que dans le cadre des fonctionnalités du présent traitement, c'est-à-dire en cas d'atteinte à la sécurité des biens ou des personnes.

Elle exclut donc l'utilisation des images par la Direction des Ressources Humaines à des fins autres que celles prévues expressément par les fonctionnalités du traitement.

Sous cette condition, les accès susvisés sont justifiés

La Commission constate par ailleurs qu'aucun accès distant (tablettes, smartphones, etc.) n'est utilisé sur le réseau de vidéosurveillance.

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.

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 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 demande que la copie ou l'extraction d'informations issues de ce traitement soit 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.

## **VII. Sur la durée de conservation**

Les informations sont conservées six mois.

A cet égard, la Commission rappelle, conformément à sa délibération n°2010-13 du 3 mai 2010, que ces informations ne peuvent être conservées sous une forme permettant l'identification de la personne concernée que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour lesquelles elles ont été collectées.

Aussi, au regard des fonctionnalités du présent traitement, elle fixe la durée de conservation des informations collectées à 1 mois.

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

**Constate** qu'aucun accès distant (tablettes, smartphones, etc.) n'est utilisé sur le réseau de vidéosurveillance.

**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 :**

- le dispositif de vidéosurveillance ne doit pas conduire à un contrôle permanent et inopportun des personnes concernées ;
- 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 ;
- l'accès aux images par la Direction des Ressources Humaines ne peut s'effectuer que dans le cadre des fonctionnalités du présent traitement, c'est-à-dire en cas d'atteinte à la sécurité des biens ou des personnes ;
- 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 chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé ;
- aucun code secret renseigné sur le distributeur automatique de billets par le client ne devra être visualisé.

**Demande** que la copie ou l'extraction d'informations issues de ce traitement soit chiffrée sur son support de réception.

**Exclut** l'utilisation des images par la Direction des Ressources Humaines à des fins autres que celles prévues expressément par les fonctionnalités du traitement.

**Fixe** la durée de conservation des informations concernant les données relatives à l'identité, aux données d'identification électronique et aux informations temporelles à 1 mois à compter de leur collecte.

**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 « *Gestion du système de vidéosurveillance des locaux* ».**

Le Président

Guy MAGNAN