Délibération n° 2021-036 du 17 février 2021

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

« *Vidéosurveillance des locaux de CFM Indosuez Wealth* »

présentée par CFM Indosuez Wealth

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 17 septembre 2020 ;

Vu la déclaration ordinaire déposée par CFM Indosuez Wealth le 7 août 2007, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Vidéosurveillance* », et dont il a été délivré récépissé le 20 août 2007 ;

Vu la demande d'autorisation déposée par CFM Indosuez Wealth le 16 novembre 2020 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Vidéosurveillance des locaux de CFM Indosuez Wealth* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 14 janvier 2021, 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 17 février 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

CFM Indosuez Wealth est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 56S00341, qui a pour objet social « *en 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 leurs sont applicables* ».

En 2007, cette société a déclaré à la Commission un traitement automatisé d'informations nominatives ayant pour finalité « *Vidéosurveillance* ». La Commission a émis un récépissé de mise en œuvre de ce traitement le 20 août 2007.

CFM Indosuez Wealth souhaite aujourd'hui remplacer le traitement initial par le présent traitement.

La Commission en prend acte.

Le traitement objet de la présente demande a pour objet d'assurer la sécurité des biens et des personnes au sein des 7 sites de CFM Indosuez Wealth sis en Principauté.

Ledit traitement 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 « *Vidéosurveillance des locaux de CFM Indosuez Wealth* ».

Les personnes concernées sont les salariés, les clients, les prospects, les prestataires externes et le public entrant dans les locaux.

Enfin, les fonctionnalités sont les suivantes :

- assurer la sécurité des locaux, des personnes et des biens au sein de l'établissement ou lors de l'utilisation des Distributeurs Automatiques de Billets (DAB) ;
- lever des doutes en cas de suspicions liées à la sécurité ;
- 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 17 septembre 2020 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 de 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 fourniture de services bancaires et de gestion du patrimoine est une activité particulièrement exposée au risque de vol de biens et de données* ».

Le responsable de traitement indique par ailleurs que CFM Indosuez Wealth est implantée sur 7 sites et compte plus de 370 collaborateurs ce qui implique une circulation importante de personnes au sein de ses locaux.

Il souligne qu'il est « *ainsi nécessaire d'assurer la protection des personnes et des biens se trouvant dans les locaux de la banque* ».

Le responsable précise par ailleurs que *« s'agissant plus particulièrement des vols de données, le dispositif de vidéosurveillance complète le dispositif de contrôle d'accès aux locaux. Les établissements bancaires sont soumis au secret bancaire et doivent protéger les données de leurs clients sous peine de poursuites pénales* ».

La Commission prend acte que le traitement n'a pas pour objectif de contrôler de manière inopportune le comportement, les habitudes et les horaires des personnes concernées.

Elle relève en outre que les caméras ne sont pas mobiles et que les fonctionnalités zoom et micro ne sont pas activées.

La Commission demande toutefois au responsable de traitement de s'assurer que l'angle de vue des caméras ne filme pas le domaine public, notamment les trottoirs et les accès aux bâtiments. Si tel est le cas, des dispositions nécessaires (repositionnement des caméras, floutage des images…) devront impérativement être prises afin que ces caméras ne filment pas le domaine public.

Elle rappelle également que sauf justification particulière (par exemple les caisses), les postes de travail des salariés ne doivent pas être filmés.

Enfin, concernant l'utilisation des distributeurs automatiques (DAB), la Commission rappelle qu'en aucun cas le code secret renseigné sur le distributeur par le client doit pouvoir être visualisé.

Sous ces conditions, elle considère donc que le traitement est justifié, conformément aux dispositions de l'article 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, visage et silhouette des personnes ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux images et au traitement ;
- 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*

Le responsable de traitement indique que l'information préalable des personnes concernées est tout d'abord effectuée par le biais d'un affichage.

Ce document 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.

Le responsable de traitement indique par ailleurs que l'information des personnes concernées s'effectue également par le biais d'une rubrique propre à la protection des données accessible en ligne et d'une procédure interne accessible en Intranet.

Ces documents n'ayant pas été joints à la demande, la Commission rappelle que ceux-ci doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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 responsable de traitement indique que le droit d'accès s'exerce par voie postale, par courrier électronique et sur place.

A cet égard, la Commission rappelle que la réponse à un droit d'accès doit s'exercer impérativement sur place et que cette réponse doit intervenir dans le mois suivant la réception de la demande.

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° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, 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***

Le responsable de traitement indique que les enregistrements sont susceptibles d'être communiqués à l'Inspection Générale et la Direction de la Déontologie pour consultation.

A cet égard la Commission rappelle qu'une telle transmission ne peut être effectuée que dans le strict cadre des fonctionnalités du présent traitement.

Les informations sont également 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.

Sous ces réserves, la Commission considère que ces transmissions sont conformes aux exigences légales.

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

Les personnes habilitées à avoir accès au traitement sont :

- les services accueil et caisse de certains sites : consultation au fil de l'eau à certaines caméras installées sur leur site ;
- le Responsable de pôle d'un site en backup du service accueil de son site : consultation au fil de l'eau à certaines caméras installées sur son site ;
- les agents de sécurité : consultation au fil de l'eau ;
- le Directeur de la Direction des Services et des Moyens Généraux (DSMG) : possibilité d'effectuer une consultation au fil de l'eau, recherche et consultation des enregistrements, extraction ;

- le Responsable Sécurité : possibilité d'effectuer une consultation au fil de l'eau, recherche et consultation des enregistrements, extraction ;
- le Directeur de la sécurité de l'information et de la continuité d'activité (RSSI) : uniquement accès en consultation aux logs de connexion du logiciel. Pas d'accès aux enregistrements ;
- le prestataire : tous droits dans le cadre de ses opérations de maintenance, y compris en extraction, uniquement en présence et sur ordre du Responsable Sécurité ou du Directeur de la DSMG.

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 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 constate par ailleurs que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception, conformément à sa 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

Le responsable de traitement indique que les logs de connexion sont conservés 1 an.

La Commission considère que cette durée est conforme aux exigences légales.

Le responsable de traitement indique en outre que les données relatives à l'identité et les informations temporelles sont conservées 60 jours.

Concernant celles-ci, 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 relatives à l'identité et celle des informations temporelles à 1 mois à compter de leur collecte.

Après en avoir délibéré, la Commission :

Constate :

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

- que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

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 la transmission des images à l'Inspection Générale et à la Direction de la Déontologie ne peut être effectuée que dans le strict cadre des fonctionnalités du présent traitement ;

- que sauf justification particulière (par exemple les caisses), les postes de travail des salariés ne doivent pas être filmés ;

- qu'en aucun cas le code secret renseigné sur le distributeur par le client doit pouvoir être visualisé ;

- que l'affichage doit comporter *a minima* un pictogramme représentant une caméra et indiquer le nom du service auprès duquel s'exerce le droit d'accès en Principauté ;

- que l'affichage doit garantir une information visible, lisible et claire de la personne concernée et être apposé à chaque entrée de l'établissement ;

- que la rubrique propre à la protection des données accessible en ligne et la procédure interne accessible en Intranet doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993 ;

- que la réponse au droit d'accès doit s'exercer uniquement sur place ;

- que les Services de Police monégasque ne pourront avoir communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

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

- 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.

Demande au responsable de traitement de s'assurer que l'angle de vue des caméras ne filme pas le domaine public, notamment les trottoirs et les accès aux bâtiments. Si tel est le cas, des dispositions nécessaires (repositionnement des caméras, floutage des images…) devront impérativement être prises afin que ces caméras ne filment pas le domaine public.

Fixe la durée de conservation des informations liées à l'identité et celle des 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 CFM Indosuez Wealth du traitement automatisé d'informations nominatives ayant pour finalité « *Vidéosurveillance des locaux de CFM Indosuez Wealth* ».**

Le Président

Guy MAGNAN