DELIBERATION N° 2011-39 DU 18 AVRIL 2011 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION SUR LA DEMANDE PRESENTEE PAR LA HSBC PRIVATE BANK (MONACO) S.A. RELATIVE A LA MISE EN ŒUVRE D'UN TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *CONTROLE D'ACCES PAR BADGE NON BIOMETRIQUE* »

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 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, modifiée, relative à la protection des informations nominatives ;

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, susvisée ;

Vu la Délibération n° 2010-43 de la Commission du 15 novembre 2010 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 demande d'autorisation déposée par HSBC PRIVATE BANK (MONACO) S.A. le 4 mars 2011 concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Sécurité des sites d'exploitation* » ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 18 avril 2011 portant examen du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

HSBC PRIVATE BANK (MONACO) S.A. est une société de droit privé exerçant à titre principal des activités bancaires et de gestion du patrimoine pour une clientèle locale et internationale.

Dans un souci de sécurité de ses collaborateurs ainsi que de ses données, ladite banque souhaite procéder à l'installation d'un système de contrôle d'accès par badge non biométrique au sein de ses locaux, répartis sur trois sites distincts de la Principauté (le Sporting, la Villa Le Dôme et l'immeuble Belle Epoque).

A ce titre, en application de l'article 11-1 de la loi n° 1.165, modifiée, du 23 décembre 1993, concernant la mise en œuvre de traitements automatisés d'informations nominatives à des fins de surveillance, HSBC PRIVATE BANK (MONACO) S.A. soumet la présente demande d'autorisation relative au traitement ayant pour finalité « *Sécurité des sites d'exploitation* ».

I – Sur la finalité et les fonctionnalités du traitement

HSBC déclare que le présent traitement a pour finalité « *Sécurité des sites d'exploitation* ».

Toutefois, la Commission relève que HSBC a soumis deux traitements ayant la même finalité, l'un étant relatif au contrôle d'accès, et l'autre à la vidéosurveillance, lequel est l'objet d'une délibération concomitante.

A cet égard, HSBC précise que ces deux systèmes sont interconnectés. En effet, il expliqué que« *les dispositifs de contrôle d'accès sont liés au système des caméras pour lui permettre d'associer spécifiquement aux portes sous vidéosurveillance l'image à la confirmation des accès sensibles demandés. Cette fonctionnalité permet de vérifier dans certains cas particulier comme l'ouverture sous contrainte mais aussi la levée de doute concernant des retours d'anomalies comme une porte laissée trop longtemps ouverte* ».

Or l'article 10-1 de la loi n° 1.165, modifiée, req uiert que les informations nominatives soient « *collectées pour une finalité déterminée, explicite et légitime* ».

Par conséquent, afin de distinguer ces deux traitements dont les finalités diffèrent, la Commission demande que la finalité du traitement objet de la présente délibération soit reformulée dans les termes suivants : « *Contrôle d'accès par badge non biométrique* ».

Par ailleurs, les personnes concernées sont l'ensemble des collaborateurs de la banque, ainsi que les intervenants extérieurs.

Enfin, les fonctionnalités sont les suivantes :

- gérer/ administrer les accès physiques de certains espaces sensibles aux personnes autorisées selon leur habilitation (au regard de leur fonction et activité dans l'entreprise) et des plages horaires définies ;
- collecter et enregistrer informatiquement les informations d'horodatage classiques émises lors de la demande d'accès de la part des utilisateurs (numéro de badge présenté, localisation du lecteur et porte, date, heure, accès autorisé ou non) ;

- archiver les informations précédentes en cas de demande d'accès, rectifications, investigations et constitutions de preuves dans le cadre d'actes frauduleux ;
- transmettre au serveur d'authentification logique l'autorisation de signature des sessions logiques sous condition que les personnes aient bien été déclarées présentes physiquement en entrée de nos locaux ;
- permettre la production de rapports synthétiques et personnalisés en fonction des éléments collectés.

Au vu de ces éléments, et sous réserve de sa reformulation, la Commission constate que la finalité du traitement est conforme aux dispositions de l'article 10-1 de la loi n° 1.165, modifiée, susvisées.

II – Sur la licéité du traitement

Pour être licite, la Commission rappelle qu'un traitement mis en œuvre à des fins de surveillance, au sens de l'article 11-1 de la loi n° 1.165, modifiée, doit être « *nécessaire à la poursuite d'un objectif légitime essentiel* » du responsable de traitement.

A cet égard, la Commission prend acte des déclarations de HSBC selon lesquelles *« l'intérêt voire l'obligation d'installer un tel système peut aujourd'hui facilement se justifier si l'on se réfère aux règles de traçabilité qui sont désormais imposées aux établissements bancaires en général, aux directives réglementaires inscrites dans les chartes bancaires et aux réclamations déposées par les assureurs de mettre tout moyen en œuvre pour se prémunir face aux risques de fraudes, de vols ou de fuites d'information confidentielle* ».

En outre, HSBC déclare que « *l'intérêt d'installer un dispositif de contrôle d'accès sur le lieu de travail est de dissuader les personnes malintentionnées de pénétrer dans des espaces non autorisées, d'identifier les tentatives d'intrusion inopinée et en dernier recours, de répondre rapidement à une alerte avérée* ».

Ainsi, si la Commission agrée que le recours par HSBC à un système de contrôle d'accès constitue *a priori* un objectif légitime essentiel au sens de l'article 11-1 précité, il convient toutefois que les libertés et droits des personnes concernées soient protégés.

A ce titre, dans le cadre de sa délibération n° 201 0-43 du 15 novembre 2010 portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail, la Commission a rappelé, d'une part, que l'exploitation de données à des fins de contrôle d'accès ne saurait donner lieu à des pratiques abusives portant atteinte aux droits des employés, des déléguées du personnel et des délégués syndicaux ; et d'autre part, que ces données ne sauraient être détournées de la finalité pour laquelle elles ont été initialement collectées.

En l'espèce, la Commission constate que les données sont collectées uniquement à des fins de contrôle d'accès, dans une perspective de sécurité des biens et des personnes.

Par conséquent, elle considère que le traitement est licite, conformément aux dispositions de l'article 10-1 de la loi n° 1.165, modifiée.

III – Sur la justification du traitement

HSBC indique que le traitement est justifié par :

- le consentement des personnes concernées ;
- l'exécution d'un contrat ou de mesures précontractuelles avec les personnes concernées ; et
- la réalisation d'un intérêt légitime poursuivi par le responsable de traitement, sans pour autant méconnaître les libertés et droits fondamentaux des individus.

En premier lieu, la Commission observe que les collaborateurs ainsi que les intervenants externes se soumettent aux règles de sécurité et d'accès aux locaux imposées par HSBC. Par conséquent, la Commission considère que le traitement est justifié par le consentement des personnes concernées.

En second lieu, la Commission relève que l'exploitation des informations nominatives des personnes concernées dans le cadre du présent traitement constitue une condition préalable et nécessaire à l'exécution par celles-ci de leurs missions ou prestations de travail. En effet, en cas de refus du traitement de ses données nominatives, la personne concernée ne sera pas admise à pénétrer dans les locaux de HSBC, ou dans certaines zones limitativement identifiés à circulation restreinte. Par conséquent, la Commission constate que le traitement est justifié par l'exécution de mesures précontractuelles avec les personnes concernées.

En troisième et dernier lieu, HSBC indique que ce traitement est justifié par la réalisation d'un intérêt légitime, sans pour autant que soient méconnus les libertés et droits fondamentaux des individus.

A ce titre, la Commission rappelle que la loi n° 1. 165, modifiée, impose ici de mettre en balance, d'une part, la poursuite d'un intérêt légitime par le responsable de traitement, et d'autre part, le respect des droits des individus. Pour conserver cet équilibre, il convient de rechercher en quoi le traitement mis en œuvre est strictement nécessaire au but recherché.

Or il ressort des déclarations de HSBC que celle-ci a mis en place une démarche préalable d'analyse des risques afin d'orienter son choix vers des technologies adaptées et proportionnées au regard de la finalité recherchée.

La technologie de contrôle d'accès par badge non biométrique est une technologie raisonnable et maîtrisée, qui ne présente pas de risque particulier pour les individus, par opposition aux dispositifs de contrôle d'accès biométriques.

Au vu de ces éléments, la Commission considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la loi n° 1.165, modifiée.

IV – Sur les informations traitées

La Commission relève que les informations nominatives objets du présent traitement sont :

- identité : nom, prénom, photographie, service, fonction, plages horaires habituellement autorisées, numéro de poste téléphonique, zones d'accès autorisées ;
- données d'identification électronique : date et heure de passage à une zone à accès restreint, identification du point de passage.

Les informations relatives à l'identité proviennent de la liste du personnel, ainsi que des intervenants externes habilités.

Par ailleurs, les données d'identification électroniques, c'est-à-dire celles relatives aux accès, proviennent du système de gestion des accès aux locaux.

En conséquence, la Commission considère que les informations collectées sont « *adéquates, pertinentes et non excessives* », conformément aux dispositions de l'article 10-1 de la loi n°1.165, modifiée.

V – Sur les droits des personnes concernées

- Sur l'exercice du droit d'accès :

La Commission observe que le droit d'accès est exercé par courrier électronique, par voie postale ou sur place. Le délai de réponse est de quinze jours.

Les droits de modification, mise à jour des données et suppression sont exercés selon les mêmes modalités.

La Commission constate ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions de la loi n°1.165, modifiée.

- Sur l'information des personnes concernées :

La Commission relève que le responsable de traitement indique que l'information préalable des personnes concernées est effectuée suivant plusieurs modalités différentes.

En premier lieu, une procédure interne accessible sur l'Intranet permet aux personnes concernées d'être averties de l'exploitation du présent traitement.

A ce titre, la Commission rappelle que cette mention doit comprendre l'ensemble des éléments requis par l'article 14 de la loi n°1.165 , modifiée.

En second lieu, en ce qui concerne les stagiaires et intérimaires, la Commission constate qu'un document spécifique leur est remis, relatif aux règles de sécurité et de surveillance de HSBC. A la réception dudit document, ceux-ci s'engagent par leur signature à en prendre connaissance et à respecter ces règles.

A la lecture de ce document, la Commission constate l'existence d'une clause d'ordre général relative à la protection des données nominatives. Toutefois, celle-ci ne précise pas la finalité des traitements, ni les destinataires des données.

Un certain nombre d'informations informations sont en revanche précisées dans le cadre de paragraphes distincts au sein du même document, respectivement intitulés « *Accès aux locaux de la banque par le système de pointage* », « *Accès aux locaux à l'intérieur de la Banque* », et « *Destinataires des données recueillies* ».

Toutefois, la Commission estime que la lecture de ces paragraphes ne permet pas aux personnes concernées d'être averties de l'existence de plusieurs systèmes de contrôle d'accès, et notamment de systèmes biométriques.

Par conséquent, elle considère que les modalités d'informations préalables desdits individus ne sont pas conformes aux exigences de l'article 14 de la loi n°1.165, modifiée, car il n'est pas fait expressément mention de la finalité des traitements exploités au titre du contrôle d'accès par HSBC.

En troisième et dernier lieu, l'information des collaborateurs est également opérée par le biais du Manuel du Personnel, remis contre signature à chacun d'entre eux. Ce Manuel comprend une clause 2.6 relative à la « *protection des données personnelles* ».

Toutefois, la Commission constate que celle-ci n'est pas conforme aux dispositions de l'article 14 susvisé.

En effet, tout d'abord, il est fait mention de la loi n° 1.240 du 2 juillet 2001 qui n'est plus en vigueur. Le Commission demande donc de modifier cette référence par la loi n° 1.165, modifiée, du 23 décembre 1993 relative à la protection des informations nominatives.

En outre, il est prévu un droit d'accès et de rectification des personnes concernées, mais pas le droit d'opposition, qu'il conviendra donc d'ajouter.

En ce qui concerne les destinataires des données, ces informations sont inscrites dans le paragraphe 1.3 relatif à « *l'Accès* », sous-paragraphe 5 « *Destinataires des données recueillies* ».

En revanche, là encore, il n'est pas fait expressément référence à la finalité des traitements. En outre, la formulation du paragraphe ne permet pas de mettre clairement en évidence l'exploitation d'informations nominatives des collaborateurs à de telles fins.

Par conséquent, la Commission demande que la finalité soit expressément ajoutée. A ce titre, dans un souci de concision, elle propose qu'elle soit précisée dans le cadre de la clause 2.6 relative à la protection des données personnelles.

Au vu de ces éléments, la Commission demande que les mentions d'information soient modifiées et complétées selon les termes susmentionnés afin d'être conforme aux exigences de l'article 14 de la loi n° 1.165, modif iée.

VI – Sur les destinataires des données

La Commission constate que les informations collectées dans le cadre du traitement sont susceptibles de faire l'objet de transferts vers plusieurs services de HSBC situés à Monaco, à savoir :

- La Direction : elle « *peut recevoir communication de rapports automatiques ou personnalisés d'anomalie ou d'accès tentés afin de déterminer si elle a lieu de lancer une investigation plus approfondie* » ;

- Le Département Sécurité Informatique : il « *reçoit communication ou lance l'édition de rapports préconfigurés ou personnalisés limités au contrôle des accès des visiteurs et prestataires externes dans une mission de veille sécuritaire des locaux limitativement identifiés comme faisant l'objet d'une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent* ».

La Commission constate ainsi que les transferts envisagés sont nécessaires à l'accomplissement des missions légitimes des services destinataires de ces données.

Ces missions sont compatibles avec la finalité et les fonctionnalités du traitement, en application des dispositions de l'article 10-1 de la loi n° 1.165, modifiée.

Au vu de ces éléments, la Commission considère donc que les transferts d'informations objets du traitement sont conformes aux exigences légales.

VII - Sur les personnes ayant accès au traitement

La Commission relève que les personnes habilitées à avoir accès au traitement sont le personnel du :

- Département Sécurité Informatique (2 collaborateurs) : inscription, modification, mise à jour, consultation, configuration, contrôle en temps réel, investigation ;
- Département Huissiers (4 collaborateurs) : inscription, modification, mise à jour, enrôlement biométrique ;
- Département Standard/ Accueil (4 collaborateurs) : inscription, modification, mise à jour ;
- Département Informatique : maintenance logiciel, archivage et sauvegarde des données ;
- Département Services Généraux (3 collaborateurs) : support intervention maintenance périphérique ;
- Sociétés de maintenance (fabricant et installateur) : maintenance logiciel et périphérique.

Ainsi, la Commission rappelle que conformément à l'article 17-1 de la loi n° 1.165, modifiée, les accès précités devront être limités à ce qui est nécessaire aux personnes susvisées « *pour les stricts besoins de l'accomplissement de leurs missions* ».

A ce titre, la Commission a pris acte des explications données par le responsable de traitement.

Elle relève également que HSBC déclare détenir une liste des personnes autorisées à avoir accès aux informations exploitées pour ces besoins, administrée par le Département Sécurité Informatique, qui est en charge de gérer les droits des personnes autorisés à avoir accès aux informations.

A cet égard, elle demande que le traitement relatif à la gestion et la traçabilité des accès et logs au Système d'Information soit soumis à l'autorisation de la Commission conformément aux dispositions de l'article 11-1 de la loi n° 1.165, modifiée.

Sous cette réserve, la Commission considère que les accès sont conformes aux dispositions de l'article 17 de la loi n° 1.165, mo difiée.

VIII - Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations n'appellent pas d'observation.

La Commission rappelle néanmoins que, conformément à l'article 17 de la loi n° 1.165, modifiée, les mesures techniques et organ isationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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.

IX – Sur la durée de conservation des données

La Commission constate que les informations nominatives collectées sont conservées pour une durée de 10 ans.

Or aux termes de la délibération n° 2010-43 du 15 novembre 2010 précitée, la Commission recommande que :

- les données relatives à l'identité des employés ne soient pas conservées au-delà de 5 ans après le départ de l'entreprise ;
- les informations relatives aux accès ne soient pas conservées plus de trois mois à compter de leur collecte.

A cet égard, HSBC explique que « *la constatation d'une infraction ou comportement répréhensible peut nécessiter de rechercher des éléments de preuve d'évènements ayant eu lieu plusieurs années auparavant. Il est donc primordial que notre Etablissement puisse conserver ces enregistrements pendant une durée raisonnable avant de les détruire. Il ne s'agit en aucun cas de conserver des éléments à l'effet de porter atteinte à la vie privée des collaborateurs ou de contrôler la qualité et la quantité de travail de ceux-ci* ».

Toutefois, la Commission rappelle qu'en application de l'article 10-1 de la loi n° 1.165, modifiée, la durée de conservation des données doit être limitée à ce qui est « *nécessaire à la réalisation de la finalité pour laquelle elles sont collectées* ».

A ce titre, elle relève que si la durée de conservation de trois mois recommandée par la Commission dans le cadre de la délibération précitée pour ce qui est des accès peut sembler courte au regard de l'enjeu sécuritaire du système de contrôle d'accès mis en place par HSBC, il n'en demeure pas moins qu'une durée de 10 ans apparaît, quant à elle, particulièrement longue.

Par ailleurs, la durée de 10 ans proposée pour les données d'identité est incohérente car elle reviendrait par exemple à exiger la suppression des données 10 ans après la date d'embauche d'un collaborateur, même si ce dernier est encore en poste dans l'entreprise. Ainsi, la durée de conservation doit donc être décomptée à partir de la date de fin des relations de travail de la personne concernée avec la banque.

Par conséquent, la Commission demande que la durée de conservation des données relatives aux accès soit réduite à 5 ans après la date dudit accès.

Par ailleurs, pour ce qui est des données relatives à l'identité, elle exige une durée de conservation de 5 ans après la fin des relations contractuelles ou conventionnelles (stagiaires) avec HSBC, conformément aux termes de la délibération n° 2010-43 susvisée.

Après en avoir délibéré :

Rappelle que :

- l'exploitation de données à des fins de contrôle d'accès sur le lieu de travail ne saurait donner lieu à des pratiques abusives portant atteinte aux droits des employés, des déléguées du personnel et des délégués syndicaux ; et d'autre part, que ces données ne sauraient être détournées de la finalité pour laquelle elles ont été initialement collectées ;

- le traitement relatif à la gestion et la traçabilité des accès et logs au Système d'Information devra être soumis à l'autorisation de la Commission dans les plus brefs délais, conformément aux dispositions de l'article 11-1 de la loi n° 1.165, modifiée ;

Demande que :

- la finalité du traitement soit reformulée dans les termes suivants : « *Contrôle d'accès par badge non biométrique* » ;

- les mentions relatives à l'information préalable des personnes concernées soient modifiées et complétées selon les termes décrits dans la présente délibération, afin d'être conformes aux exigences de l'article 14 de la loi n° 1.165, modifiée ;

- la durée de conservation des données relatives aux accès soit réduite à 5 ans après la date dudit accès ;

- la durée de conservation des données d'identité soit réduite à 5 ans après la fin des relations professionnelles avec HSBC, conformément aux termes de la délibération n° 2010-43 du 15 novembre 2010 ;

- la liste nominative des personnes ayant accès au traitement, visée à l'article 17-1 de la loi n° 1.165, modifiée, soit tenue à jour et puisse lui être communiquée à première réquisition ;

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 HSBC PRIVATE BANK (MONACO) S.A. du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle d'accès par badge non biométrique* ».**

Le Président,

Michel SOSSO