DELIBERATION N° 2011-37 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 « *SECURITE DES SITES D'EXPLOITATION PAR VIDEOSURVEILLANCE* »

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° 2010-13 de la Commission du 3 mai 2010 portant recommandation sur les dispositifs de vidéosurveillance mis en œuvre par les personnes physiques ou morales de droit privé ;

Vu l'autorisation délivrée par le Ministre d'Etat en date du 22 décembre 2010 ;

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 vidéosurveillance 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

Le présent traitement a pour finalité « *Sécurité des sites d'exploitation* ». La dénomination du traitement est « *Sécurité des sites d'exploitation par vidéosurveillance* ».

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

Le responsable de traitement précise que ces deux systèmes sont interconnectés. En effet, il déclare qu'« *au niveau de l'interface utilisateur de l'historique des évènements du système de contrôle d'accès, une personne disposant du droit d'accès sera capable, en double-cliquant sur un événement, de faire apparaître la vidéo associée, dans le cas où une caméra a le point de contrôle d'accès dans son champs visuel* ». Cette interconnexion permet de renforcer la sécurité de la banque.

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 « *Sécurité des sites d'exploitation par vidéosurveillance* ».

Par ailleurs, les personnes concernées sont l'ensemble des collaborateurs de la banque, ainsi que des clients et visiteurs professionnels.

Enfin, les fonctionnalités sont les suivantes :

- assurer la sécurité des personnes ;
- assurer la sécurité des biens de la banque ;
- renforcer le contrôle des accès, et notamment procéder à des contrôles sur la circulation des personnes extérieures à la banque dans les locaux sur les trois sites de la banque, par le biais d'une interconnexion avec le système de contrôle d'accès, objet d'une demande d'autorisation concomitante ;
- constituer des preuves en cas d'infractions ;
- globalement, minimiser les risques de vol de toute nature.

A cet égard, HSBC déclare que « *l'objectif n'est en aucune manière de contrôler le travail des salariés sur les plans qualitatif (concentration/ vitesse d'exécution…) et quantitatif (horaires)* ».

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

II - Sur la licéité du traitement

La Commission rappelle que l'exercice sur le territoire monégasque d'une activité privée de surveillance accomplie en vue d'assurer la sécurité des personnes est soumis aux dispositions de la loi n° 1.264 du 23 décembre 2002 relative aux activités privées de protection des personnes et des biens.

A ce titre, la Commission constate que HSBC a préalablement obtenu l'autorisation du Ministre d'Etat, en application des articles 5 et 6 de ladite loi.

Or, dans le cadre de sa délibération n°2010-13 du 3 mai 2010 portant recommandation sur les dispositifs de vidéosurveillance mis en œuvre par les personnes physiques ou morales de droit privé, la Commission a estimé que l'obtention de l'autorisation susvisée attestait du caractère licite de l'activité de surveillance, ainsi que des moyens utilisés à cette fin.

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 la réalisation d'un intérêt légitime poursuivi par le responsable de traitement, sans que soient méconnus les libertés et droits fondamentaux de la personne concernée.

A ce titre, à l'aune du principe de proportionnalité posé par la Cour Européenne des Droits de l'Homme[1], la Commission rappelle que l'article 10-2 de la loi n°1.165, modifiée, impose de mettre en balance, d'une part, l'intérêt légitime du responsable de traitement, et d'autre part, les libertés et droits fondamentaux des personnes concernées par le traitement.

En l'espèce, HSBC fournit les explications suivantes :

« *HSBC Private Bank (Monaco) SA est aujourd'hui la banque n°1 sur Monaco, avec plus de 200 salariés, implantée sur 3 sites. Cela implique de nombreuses circulations de collaborateurs, de consultants et de prestataires de services sur les 3 sites et à l'intérieur des 3 sites*

L'activité bancaire est basée sur le développement d'un fonds de commerce dont les données clientèle sont l'actif majeur. Pour protéger les clients et la Banque, la Principauté a prévu des sanctions pénales à toute violation du secret bancaire. Le groupe HSBC a été victime récemment d'un vol de données de la clientèle, qui lui a été préjudiciable vis à vis de la clientèle existante et en termes de réputation. Toute violation du secret bancaire en

[1] Voir par exemple : CEDH, Klass & autres c. Allemagne, 6 septembre 1978 ; Leander c. Suède, 26 mars 1987 ; Niemietz c. Allemagne, 16 décembre 1992 ; Marper c. Royaume-Uni, 4 décembre 2008.

Principauté, notamment par le vol de données, serait extrêmement préjudiciable pour l'image de marque de la Principauté et le développement de son secteur bancaire.

La sécurité des personnes (collaborateurs et clients) et des biens justifie aujourd'hui l'installation d'un système de vidéosurveillance ».

Si ces déclarations illustrent effectivement un intérêt légitime du responsable de traitement tendant à la sécurité des personnes et des biens, et à la prévention du vol de données, la Commission constate néanmoins que l'étendue de l'exploitation visée est susceptible de porter atteinte aux libertés et droits fondamentaux des personnes concernées.

En effet, la Commission observe que le système de vidéosurveillance a vocation à couvrir les espaces suivants : open spaces, salles informatiques, baies de brassage, entrées/ sorties des bâtiments (livraison et public), guichets et caisses, halls d'accueil, couloirs, parkings.

Or, malgré les affirmations du responsable de traitement selon lesquelles « *l'objectif n'est en aucune manière de contrôler le travail des salariés sur les plans qualitatif (…) et quantitatif (…)* », la Commission considère que l'installation d'un système de vidéosurveillance dans les open spaces est disproportionnée au regard de la finalité du traitement, dans la mesure où il conduit intrinsèquement à une surveillance permanente et inopportune des employés.

Cette surveillance est d'autant plus importante que le dispositif permet d'interagir avec les caméras en zoomant ou en déplaçant le champ de vision des caméras, comme l'indique le responsable de traitement.

Aussi, la Commission tient à rappeler les Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance, adoptés par le Comité Européen de Coopération Juridique du Conseil de l'Europe les 20-23 mai 2003.

Ainsi, le Conseil de l'Europe préconise :

- « *de limiter le recours à des systèmes de vidéosurveillance sur le lieu de travail à des exigences organisationnelles et/ou de production, ou à des fins de sécurité au travail. Ce système ne doit pas avoir pour but de la surveillance délibérée et systématique de la qualité et de la quantité du travail individuel sur le lieu de travail* » ;

- « *de recourir à la vidéosurveillance de manière adéquate, pertinente et non excessive par rapport aux finalités déterminées et spécifiques recherchées dans les cas individuels, lorsque le besoin en a été démontré, afin d'éviter toute atteinte inconsidérée et injustifiée aux droits et libertés fondamentales des personnes concernées* » ;

- « *de n'utiliser la vidéosurveillance que si, selon les circonstances, la finalité de cette dernière ne peut être atteinte par d'autres mesures portant moins atteinte au respect de la vie privée (…)* ».

En l'espèce, HSBC souhaite mettre en place un système de sécurité particulièrement complet aux fins, notamment, de se prémunir contre le vol de données. Ce système comprend un dispositif de contrôle d'accès physique aux locaux et à certaines zones de circulation restreinte à l'intérieur des locaux, couplé à un système de vidéosurveillance ainsi que de gestion des accès au système informatique et de traçabilité des logs.

Ainsi, la Commission constate que :

- HSBC a d'ores et déjà prévu un certain nombre de mesures de sécurité moins attentatoires aux droits et libertés fondamentales des personnes concernées (contrôle d'accès, gestion et traçabilité des accès informatiques) ;

- un système de vidéosurveillance limité à la surveillance des couloirs d'accès aux open spaces semblerait suffisant au regard de la finalité du traitement.

En outre, la Commission relève que le fait que les enregistrements vidéo ne se déclenchent que sur évènement est sans effet sur le caractère disproportionné du dispositif, puisque les évènements dans les open spaces surviennent en permanence.

Le principe intangible interdisant la surveillance permanente des employés sur le lieu de travail a donc été expressément réitéré par la Commission dans le cadre de la délibération n°2010-13 précitée.

La Commission a en effet estimé que « *l'installation d'un système de vidéosurveillance est strictement interdit dans (…) les bureaux, ainsi que tous les lieux privatifs mis à la disposition des salariés à des fins de détente ou de pause-déjeuner* ».

Au vu de l'ensemble de ces éléments, la Commission constate que :

- le système de vidéosurveillance que HSBC souhaite mettre en place dans les open spaces est disproportionné au regard de la finalité à atteindre, en ce qu'il aboutit à une surveillance permanente et excessive des collaborateurs ;

- les explications apportées par HSBC ne sont pas de nature à justifier l'atteinte portée aux libertés et droits fondamentaux des collaborateurs.

En conséquence, la Commission considère que la justification du traitement objet de la présente demande d'autorisation n'est pas conforme aux dispositions de l'article 10-2 de la loi n°1.165.

Elle invite le responsable de traitement à trouver une solution alternative non attentatoire des libertés et droits fondamentaux des individus, telle que la mise en place d'une vidéosurveillance des couloirs d'accès aux open spaces, plutôt que des open spaces eux-mêmes.

Par ailleurs, en ce qui concerne le reste du dispositif de vidéosurveillance (salles informatiques, caisses, etc.), la Commission estime que la justification apportée par HSBC est conforme à l'article 10-2 susvisé.

Elle rappelle néanmoins que les caméras employées dans les zones ouvertes au public devront demeurées de type fixe et sans zoom, comme c'est le cas actuellement d'après l'Annexe 11 E fournie par le responsable de traitement.

IV - Sur les informations traitées

Les informations nominatives objets du présent traitement sont :

- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès au traitement ;

- images des collaborateurs : enregistrement des mouvements de personnel dans les bureaux ;
- informations de localisation et horodatage: les images enregistrées seront horodatées et présenteront l'identification de la caméra repérée sur les plans.

Toutefois, la Commission constate que des informations complémentaires sont collectées, à savoir l'image des clients et visiteurs professionnels de HSBC. Il conviendrait donc de les ajouter au titre des informations collectées dans le cadre du traitement objet de la présente délibération.

Par ailleurs, l'ensemble de ces informations a pour origine le système de vidéosurveillance lui-même.

Enfin, la Commission rappelle que l'article 10-1 de la loi n°1.165, modifiée, exige que les informations nominatives soient « *adéquates, pertinentes et non excessives au regard de la finalité pour laquelle elles sont collectées et pour laquelle elles sont traitées ultérieurement* ».

Or, considérant le caractère disproportionné de la vidéosurveillance des open spaces déjà évoqué par la Commission dans le cadre de la présente délibération, il en ressort que la collecte des images des collaborateurs dans lesdits open spaces est nécessairement inadéquate et excessive, en violation des dispositions de l'article 10-1 précité.

En revanche, en ce qui concerne les autres données objets du traitement (images des personnes concernées en dehors des open spaces et bureaux), la Commission considère que celles-ci sont conformes 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. Le délai de réponse est de trente 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 1.165, modifiée.

- Sur l'information des personnes concernées :

La Commission observe que l'information préalable des personnes concernées est effectuée suivant deux modalités différentes.

En premier lieu, un affichage sous la forme d'un autocollant est visible à l'entrée des locaux ainsi que dans toutes les parties communes de la banque. Il comprend un pictogramme représentant une caméra, ainsi que l'indication « *Etablissement sous vidéosurveillance* » inscrite dans trois langues (français, anglais, italien). Enfin, l'affichage indique : « *Exercice du droit d'accès, de rectification et d'opposition à transmettre auprès de la Direction de HSBC Private Bank (Monaco) SA* ».

Cet affichage est donc conforme aux termes de la délibération n°2010-13, précitée.

En second lieu, la Commission relève que l'information préalable des personnes est également effectuée par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé.

En l'espèce, il s'agit de mentions inscrites dans le « *Manuel du Personnel* ».

En conséquence, elle constate que le personnel est informé, au travers dudit Manuel, de l'ensemble des éléments imposés par l'article 14 de la loi n°1.165, modifiée.

Au vu de ces éléments, la Commission considère que les personnes concernées sont dûment avertis, conformément aux dispositions de l'article 14 susvisé.

VI – Sur les destinataires des informations

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 :

- le service Contrôle interne, dans le cadre de l'audit périodique du bon fonctionnement du système de vidéosurveillance ;

- le service juridique, en cas de litige avec un client ou visiteur professionnel ou de demande des autorités judicaires justifiant la visualisation des images stockées ;

- les Ressources Humaines, en cas de litige avec un membre du personnel ou prestataire externe ;

- la Direction, pour toutes les raisons citées ci-dessus ;

- l'Auditeur interne Groupe, pour vérifier le bon fonctionnement du système.

En outre, la Commission prend acte des déclarations du responsable de traitement aux termes desquelles « *les images [enregistrées] pourront être communiquées aux services ci-dessus sous format de courrier électronique* ».

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 constate que les personnes habilitées à avoir accès au traitement sont le personnel du :

- Département Sécurité Informatique (2 collaborateurs) : consultation uniquement ;
- Département Huissiers (4 collaborateurs) : consultation uniquement ;
- Département Informatique : tous droits.

A ce titre, 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* ».

Ainsi, 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.

Enfin, elle rappelle que conformément à la délibération n°2010-13 précitée, la possibilité d'interagir avec les caméras ne devrait en aucun cas conduire à surveiller des zones pour lesquelles la vidéosurveillance est illicite, et notamment les open spaces, les bureaux, et les espaces de détente du personnel.

Au vu de ces éléments, la Commission considère que les accès sont conformes aux dispositions des articles 17 et 17-1 de la loi n°1. 165, modifiée.

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 organisationnelles 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

La Commission constate que les informations nominatives collectées sont conservées pour une durée d'un an en ce qui concerne les logs de connexion au système de vidéosurveillance, et de 6 mois en ce qui concerne les images des personnes concernées et les informations de localisation et d'horodatage.

Elle relève que ces durées de conservation sont plus longues que la durée d'un mois proposée dans le cadre de la délibération n° 2010-1 3, précitée.

A cet égard, HSBC souhaite faire valoir le caractère particulièrement sensible des données traitées, et appelle l'attention de la Commission sur le vol de données dont le groupe HSBC a déjà été victime et qui a fait grand bruit dans la presse en 2010. Elle évoque la grave atteinte que cela représente pour la réputation de la banque, mais également pour la vie privée de ses clients.

En outre, la Commission prend acte des déclarations de HSBC aux termes desquelles « *la recherche d'éléments de preuves concernant un comportement suspect ou une infraction peut fréquemment intervenir plusieurs mois après la survenance de ces faits. Il est donc primordial que notre Etablissement puisse conserver ces enregistrements pendant une durée raisonnable avant de les détruire* ».

Or, si la Commission ne peut transiger sur la possibilité de procéder à une vidéosurveillance constante des bureaux et open spaces, elle peut toutefois admettre une durée de conservation plus longue que celle prévue dans le cadre de la délibération n°2010-13, si le responsable de traitement évoque des justifications particulières, ce qui est le cas en l'espèce.

Au vu de ces éléments, la Commission considère donc que la durée de conservation est conforme aux exigences légales.

Après en avoir délibéré :

Rappelle que :

- les informations nominatives collectées doivent être « *pertinentes, adéquates et non excessives* » en application de l'article 10-1 de la loi n° 1. 165, modifiée ;

- l'article 10-2 de la loi n° 1.165, modifiée, impose de mettre en balance, d'une part, l'intérêt légitime du responsable de traitement et, d'autre part, les libertés et droits fondamentaux des personnes concernées, conformément au principe de proportionnalité posé par la Cour Européenne des Droits de l'Homme ;

- 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 ;

Considère que :

- la vidéosurveillance des open spaces et de tout espace de bureau est disproportionné au regard de la finalité du traitement, en ce qu'elle conduit à une surveillance permanente et inopportune des employés ;

- la collecte des images des personnes concernées dans les espaces précités n'est pas conforme aux dispositions de l'article 10-1 de la loi n° 1.165, modifiée ;

- un tel traitement, bien que justifié par la réalisation d'un intérêt légitime du responsable de traitement, porte atteinte aux libertés et droits fondamentaux des personnes concernées, en violation des dispositions de l'article 10-2 de la loi n° 1.165, modifiée ;

Demande que :

- la finalité du traitement soit reformulée dans les termes suivants : « *Sécurité des sites d'exploitation par vidéosurveillance* » ;

- la vidéosurveillance soit limitée aux salles informatiques, baies de brassage, entrées/ sorties des bâtiments (livraison et public), guichets et caisses, halls d'accueil, couloirs, parkings, à l'exclusion des open spaces et tout autre espace de bureau ;

- la typologie de caméras employées dans les zone ouvertes au public demeure fixe et sans zoom, afin de limiter l'atteinte à la vie privée ;

- 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 « *Sécurité des sites d'exploitation par vidéosurveillance* ».**

Le Président,

Michel SOSSO