Délibération n° 2023-070 du 17 mai 2023

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

« *Contrôle d'accès grâce à un dispositif de reconnaissance biométrique de l'iris* »

présenté par Pictet & Cie (EUROPE) S.A.

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 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007, modifiée, portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée, 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 l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers ;

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 la délibération n° 2011-33 du 11 avril 2011 portant recommandation sur les dispositifs biométriques reposant 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 les personnes physiques ou morales de droit privé ;

Vu la demande d'autorisation déposée par Pictet & Cie (EUROPE) S.A. le 23 janvier 2023 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Contrôle d'accès grâce à un dispositif de reconnaissance biométrique de l'iris* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 22 mars 2023, 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 mai 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Pictet & Cie (EUROPE) S.A. est une société étrangère, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 19S08324 ayant entre autres pour objet en Principauté « *La gestion, pour le compte de tiers, de portefeuilles de valeurs mobilières ou d'instrument financiers à terme ; la réception et la transmission d'ordres sur les marchés financiers, portant sur des valeurs mobilières ou des instruments financiers à termes, pour le compte de tiers ; le conseil et l'assistance : dans la gestion, pour le compte de tiers, de portefeuilles de valeurs mobilières ou d'instruments financiers à terme ; dans la réception et la transmission d'ordres sur les marchés financiers, portant sur des valeurs mobilières ou des instruments financiers à terme, pour le compte de tiers* ».

Afin de contrôler l'accès à ses locaux et à certaines zones restreintes desdits locaux, elle souhaite mettre en place un système biométrique reposant sur la reconnaissance de l'iris exclusivement enregistrée sur un support individuel détenu par la personne concernée.

Le traitement objet de la présente 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 responsable de traitement indique que traitement dont s'agit a pour finalité « *Contrôle d'accès grâce à un dispositif de reconnaissance biométrique de l'iris* ».

Les personnes concernées sont les salariés et les stagiaires.

Enfin, les fonctionnalités du traitement sont :

- contrôler l'accès aux locaux de l'établissement et à des zones restreintes des locaux ;
- assurer le respect du secret professionnel ;
- assurer la sécurité des personnes et des biens ;

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

Le responsable de traitement indique que le présent traitement est justifié tout d'abord par l'exécution d'un contrat ou de mesures précontractuelles avec la personne concernée puisqu'« *Il vise à s'assurer que seules les personnes répondant à ce statut peuvent librement entrer dans les locaux et dans certaines zones de l'établissement* ».

Il précise par ailleurs que *« l'un des objectifs est la protection des espaces les plus sensibles de l'entreprise, dont les salles serveurs et télécom, ainsi que le fichier central contenant l'ensemble des données de la Banque et des clients* ».

Le responsable indique que le traitement est également justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement qui ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission note ainsi que « *De manière générale, ce traitement vise la mise en place de mesures de sécurité physique (ajout d'un facteur d'identification) et de garantir le respect du secret professionnel visé à l'article 308 du code pénal qui concerne toutes les données collectées, traitées et stockées dans le cade des autres traitements de la Banque* ».

Elle relève également que « *L'empreinte biométrique est inscrite sur une carte RFID qui est en possession de l'employé* », qu'elle « *n'est pas stockée/gardée sur aucune des infrastructures de la banque* » et qu'« *En cas de perte de la carte RFID, il est nécessaire de refaire* » une procédure d'enrôlement.

Enfin, la Commission prend acte que « *Le dispositif n'a en aucune manière pour finalité de contrôler les horaires de travail* ».

Elle attire toutefois l'attention du responsable de traitement sur le fait qu'à l'instar de l'empreinte digitale, l'iris n'est pas une donnée comme les autres. Elle n'est en effet pas attribuée par un tiers ou choisie par la personne concernée mais provient de son corps et la désigne de façon définitive. Le détournement d'une telle donnée peut donc avoir des conséquences graves.

La Commission souligne enfin 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, elle 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, numéro de profil ;
- données d'identification électronique : login, mot de passe de l'application ;
- donnés biométriques : gabarit de l'iris ;
- données temporelles : heure et jour de passage ;
- informations spatio-temporelles : zone et heure d'accès ;
- numéro du badge.

Les informations relatives à l'identité ont pour origine la personne concernée et le traitement.

Toutes les autres informations ont pour origine le système biométrique.

La Commission constate ainsi 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 des personnes concernées s'effectue par le biais d'un document spécifique.

A cet égard, la Commission rappelle que ce document doit impérativement comporter l'ensemble des mentions prévues 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 responsable de traitement indique que le droit d'accès s'exerce sur place ou par courrier électronique auprès du COO (Chief Operating Officer) ou DPO Europe.

A cet égard, la Commission rappelle que la réponse à un droit d'accès 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° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous cette condition, elle 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 toutes les informations, à l'exception des données biométriques, 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***

Les personnes ayant accès au traitement sont :

- le Chief Operating Officer : consultation uniquement sur autorisation du Management du département de la sécurité Physique du Groupe ;
- l'administrateur réseau : gestion de la base de données, sans faculté de supprimer ou altérer les données.

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

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 les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'un rapprochement avec le traitement ayant pour finalité « *Gestion administrative des salariés* », légalement mis en œuvre.

La Commission considère que ce rapprochement est conforme aux exigences légales.

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.

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

La Commission 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 les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité sont conservées pendant toute la durée de l'habilitation.

La photo de l'iris est immédiatement supprimée après sa conversion en un gabarit numérique de 32 chiffres.

Le gabarit est quant à lui conservé le temps de l'habilitation.

Enfin, le responsable de traitement indique que les données d'identification électronique, les informations temporelles, les informations spatio-temporelles et le numéro de badge sont conservés 12 mois glissants après le passage.

A cet égard, la Commission rappelle que conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, ne peuvent être conservées sous une forme permettant l'identification de la personne que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité du traitement.

Aussi, elle fixe la durée de conservation des données temporelles et des informations spatio-temporelles à 3 mois à compter du dernier passage.

Enfin, la Commission considère que le numéro de badge est quant à lui conservé pendant toute la durée de l'habilitation.

Après en avoir délibéré, la Commission :

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 :

- l'information préalable des personnes concernées doit impérativement comportée l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

- la Direction de la Sûreté Publique ne pourra avoir communications des informations objet du traitement, que dans le strict cadre de ses missions légalement conférées ;

- 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.

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

Fixe la durée de conservation des données temporelles et des informations spatio-temporelles à 3 mois à compter du dernier passage.

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 Pictet & Cie (EUROPE) S.A. du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle d'accès grâce à un dispositif de reconnaissance biométrique de l'iris* ».**

Le Président

Guy MAGNAN