Délibération n° 2017-204 du 15 novembre 2017

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

« *Authentification de l'identité des clients et de leurs représentants par un dispositif biométrique de reconnaissance vocale* »

présenté par Barclays Bank PLC (Succursale de Monaco)

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 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 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'Ordonnance Souveraine n° 3.559 du 5 décembre 2011 rendant exécutoire l'Accord monétaire entre l'Union européenne et la Principauté de Monaco ;

Vu l'Ordonnance Souveraine n° 5.713 du 8 février 2016 modifiant les annexes de l'Accord monétaire conclu le 29 novembre 2011 entre l'Union européenne et la Principauté de Monaco ;

Vu l'Arrêté français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution ;

Vu la demande d'autorisation présentée le 29 août 2017 par Barclays Bank PLC (Succursale de Monaco), concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Lutte contre la fraude interne et externe* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation modificative notifiée au responsable de traitement le 27 octobre 2017, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 15 novembre 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Barclays Bank PLC est une banque anglaise (Londres) établie à Monaco par le biais de sa succursale enregistrée au RCI sous le numéro 68S01191, et ayant pour activité : « *la réalisation de toutes opérations de banque et connexes, telles que définies par la Loi bancaire* ».

Afin de prévenir certains types de fraudes reposant notamment sur l'usurpation d'identité, elle souhaite proposer à ses clients une méthode d'authentification alternative par reconnaissance vocale.

Le traitement objet de la présente demande comporte des données biométriques nécessaires au contrôle de l'identité des personnes. Il est donc soumis au régime de l'autorisation de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Lutte contre la fraude interne et externe ».*

Le responsable de traitement indique qu'il concerne « *les clients et leurs représentants ayant consentis au service et les employés volontaires pour le paramétrage de l'outil* ».

Les fonctionnalités du traitement sont les suivantes :

« *Le système Voice Security a pour objectif de permettre au personnel habilité (banquiers privés et leurs assistants, digital & Client Services…) de vérifier l'identité des clients de la banque lors d'une conversation téléphonique, d'une manière simple et sécurisée.*

Les principales fonctionnalités sont :

- *enrôlement : création d'un gabarit d'empreinte vocale associé à un profil client unique, stockage et archivage des données biométriques relatives aux clients pour permettre l'exploitation du système Voice Security ;*
- *vérification : identification et authentification des clients par comparaison de la voix de l'appelant à l'enregistrement vocal préalablement enregistré et archivé ».*

Aussi le responsable de traitement précise que :

- « *ceci est rendu possible par la liaison du système téléphonique de Barclays (…) avec le serveur comprenant le logiciel d'administration du contrôle (Voice Security) implémenté sur l'ensemble des postes des salariés de Barclays du Front Office en relation avec la clientèle et autorisés à pouvoir le faire* » ;
- le « *serveur sur lequel est stocké le logiciel d'exploitation des empreintes vocales des clients de Barclays Monaco (…) est hébergé dans les locaux de Barclays Monaco* » ;
- « *les données biométriques stockées sont chiffrées* ».

A cet égard, la Commission prend acte, d'une part, que « *le gabarit d'empreinte vocale (…) est irréversible et il est impossible de reproduire ni de constituer la voix du client à partir de celui-ci* », et d'autre part, que « *Barclays a mis en place un dispositif de détection du rejeu* » afin d'endiguer des attaques par usurpation d'identité.

Par ailleurs, elle observe que la finalité envisagée ne traduit pas le but d'authentification des clients et de leurs représentants au moyen d'un dispositif biométrique de reconnaissance vocale.

Aussi, la Commission considère qu'il convient de reformuler la finalité proposée, conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993, lequel dispose que les informations nominatives doivent être collectées pour une finalité déterminée, explicite et légitime.

En conséquence, elle modifie comme suit la finalité du traitement dont s'agit : « *Authentification de l'identité des clients et de leurs représentants par un dispositif biométrique de reconnaissance vocale* ».

II. Sur la licéité et la justification du traitement

➢ *Sur la licéité du traitement*

La Commission observe que les risques de fraude interne et externe sont inclus dans la définition du risque opérationnel tel qu'énoncé au j de l'article 10 de l'Arrêté français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution (applicable à la Principauté de Monaco dans les limites de son article 275) et que l'article 94 dispose que « *les entreprises assujetties mettent en place des systèmes d'analyse et de mesure des risques en les adaptant à la nature et au volume de leurs opérations afin d'appréhender les risques de différentes natures auxquels ces opérations les exposent, et notamment (…) le risque opérationnel* ».

Aussi, le point j de l'article 10 de l'Arrêté français du 3 novembre 2014 le décrit ainsi que suit :

« *j) Risque opérationnel : conformément au 52 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 susvisé, le risque de pertes découlant d'une inadéquation ou d'une défaillance des processus, du personnel et des systèmes internes ou d'événements extérieurs, y compris le risque juridique ;*

Le risque opérationnel inclut notamment les risques liés à des événements de faible probabilité d'occurrence mais à fort impact, les risques de fraude interne et externe définis à l'article 324 du règlement (UE) n° 575/2013 susvisé, et les risques liés au modèle ».

L'article 324 du règlement (UE) n° 575/2013 (mentionné à l'Annexe A de l'Accord monétaire conclu le 29 novembre 2011 entre l'Union européenne et la Principauté de Monaco) les décrit ainsi que suit :

« *Fraude interne : Pertes liées à des actes visant à commettre une fraude ou un détournement d'actif ou à enfreindre/tourner une réglementation, une loi ou des règles de l'entreprise, à l'exclusion des cas de discrimination ou d'inapplication des règles en matière de diversité, et impliquant au moins un membre de l'entreprise.*

Fraude externe : Pertes liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif ou à enfreindre/tourner la loi (…) ».

Ainsi, la Commission considère que le traitement dont s'agit met en œuvre un dispositif contribuant à la limitation des risques opérationnels en tant que la prévention contre le risque d'usurpation d'identité participe à l'évidence à la lutte contre de telles fraudes.

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

- ***Sur la justification***

Le responsable de traitement indique que le traitement dont s'agit est justifié par le consentement des personnes concernées et la réalisation d'un intérêt légitime poursuivi par le responsable de traitement et ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

Sur la première justification tenant au consentement des personnes concernées, il précise qu'« *un processus strict est mis en place pour s'en assurer. Pour les employés, dont l'empreinte vocale est utilisée pour le paramétrage et les tests de l'outil, la participation est basée sur le volontariat. Le processus d'enrôlement est divisé en 5 phases, visant à assurer que, préalablement à tout enregistrement de gabarit, les personnes concernées ont eu toutes les informations nécessaires et ont donné un accord réfléchi et en connaissance de cause* ».

La documentation jointe aux fins d'illustration du consentement des clients n'appelle pas de remarque de la Commission qui constate par ailleurs que le client :

- bénéficie d'une information individualisée ;
- d'un délai de réflexion minimum de 5 jours ;
- peut à tout moment demander l'annulation de son enrôlement au Service VoiceSecurity.

Sur la seconde justification, il précise que « *dans l'optique de préserver les avoirs des clients, Barclays a entrepris de se doter de cette technologie capable de reconnaître l'empreinte vocale de ses clients afin de déceler automatiquement les cas de fraude par usurpation d'identité* ».

Aussi la Commission considère 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 traitées

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité/situation de famille : nom, prénom, date et lieu de naissance, genre, nationalité, statut marital, numéro de carte d'identité ou de passeport ;
- adresses et coordonnées : adresse, numéros de téléphone fixes et mobiles ;
- caractéristiques financières : nom et localisation du banquier, parties associées, numéros de comptes, catégorie de risque, dernière transaction ;
- données d'identification électroniques : adresse email, identifiant électronique ;
- données biométriques : gabarit de l'empreinte vocale ;
- informations temporelles : date et heure de la création du gabarit, historique d'utilisation du gabarit ;
- autres données collectées : statut du consentement, langue choisie, enregistrements vocaux.

Il précise que les informations temporelles sont issues du système VoiceSecurity, celles relatives à l'identité/situation de famille, aux adresses et coordonnées, aux caractéristiques financières et les données d'identification électroniques ont pour origine le traitement ayant pour finalité « *la tenue des comptes de la clientèle afin de proposer des services bancaires* », et les autres informations proviennent de la personne concernée.

Par ailleurs, à l'examen du dossier, il apparaît que « *l'échantillon de voix utilisé pour créer le gabarit d'empreinte vocale est crypté et stocké à des fins de paramétrage de l'outil dans un répertoire sécurisé, séparément du gabarit* ».

De même, la Commission constate que le traitement dont s'agit fait l'objet d'une journalisation (date/heure de connexion, identifiant de l'utilisateur, opération effectuée).

Enfin, elle relève également que l'application Voice Security permet au personnel habilité de la banque d'enregistrer le consentement du client ainsi que la langue choisie et de suivre l'historique d'enrôlement de chaque client concerné.

La Commission prend donc acte de ces éléments.

Aussi, la Commission considère 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 assurée au moyen d'une procédure interne accessible en Intranet, d'un courrier adressé à l'intéressé et d'autre séance obligatoire d'explication et de questions/réponses par téléphone.

A l'examen des éléments joints au dossier, la Commission relève que si le processus d'enrôlement est largement décrit, elle n'est cependant pas en mesure de s'assurer de la qualité de l'information préalable des personnes concernées au sens de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

En conséquence, la Commission demande que le responsable de traitement s'assure de l'information préalable de l'ensemble des personnes concernées et qu'elle soit conforme à 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 les droits d'accès, de modification, de mise à jour et de suppression s'exercent par voie postale auprès du Dirigeant Effectif de Barclays Bank PLC (Succursale de Monaco).

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit intervenir dans le mois suivant la réception de la demande.

Elle constate ainsi 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. <u>Sur les personnes ayant accès au traitement et les communications d'informations</u>

- ***Sur les accès au traitement***

Le responsable de traitement indique qu'ont accès au traitement :

- S'agissant de l'accès au serveur Voice Security contenant les gabarits, le Département Informatique : en maintenance, et les Services d'audit et de contrôles : en consultation.

- S'agissant des accès et utilisation de l'application Voice Security :
  - Front Office, Equipe Client Services (pour l'enrôlement client et la reconnaissance vocale) : en inscription et consultation ;
  - Equipe Digitale (en charge du déploiement de l'outil) : en inscription et consultation ;
  - Département Informatique : en maintenance ;
  - Département GI&S (global Investment and Solutions) – traders (pour la reconnaissance vocale des clients : en consultation ;
  - Services d'audit et de contrôle : en consultation.

Par ailleurs, il précise que « *toutes les équipes ci-dessus font partie de Barclays Bank Plc (Succursale de Monaco)* » et que *« seuls les champs « choix de la langue » et « consentement » peuvent être modifiés par les équipes ayant des droits d'inscription* ».

Aussi, la Commission souligne qu'en cas de recours à des prestataires, leurs accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993. De plus ils sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement.

Elle 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.

Elle considère que ces accès sont justifiés.

- ***Sur les communications d'informations***

Le responsable de traitement n'indique pas d'autre communication d'informations qu'au sein de Barclays Bank Plc Succursale de Monaco.

Aussi, la Commission rappelle qu'elles sont susceptibles d'être communiquées aux Autorités compétentes dans le cadre des missions qui leurs sont légalement conférées.

VI. Sur les rapprochements et les interconnexions avec d'autres traitements

Le responsable de traitement indique un rapprochement avec les traitements ayant pour finalité respective « *la tenue des comptes de la clientèle afin de proposer des services bancaires*» et « *système d'habilitation* ».

A cet égard, la Commission observe, d'une part, que le traitement se rapportant au « *système d'habilitation* » n'a pas été légalement mis œuvre et d'autre part qu'il est effectué a minima une journalisation des accès au traitement dont s'agit.

En outre, elle relève l'existence d'une « *liaison du système téléphonique de Barclays avec le serveur comprenant le système d'administration du contrôle (VoiceSecurity) implémenté sur l'ensemble des postes des salariés de Barclays du Front Office en relation avec la clientèle (…)* ».

Elle en déduit donc une interconnexion avec un traitement relatif à la gestion des services de téléphonie fixe et/ou mobile sur le lieu de travail.

Aussi, la Commission demande que les traitements relatifs à la gestion des accès et des habilitations et à la gestion des services de téléphonie fixe et/ou mobile sur le lieu de travail, lui soient soumis dans les plus brefs délais.

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.

Cependant les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

La Commission rappelle que si des informations du traitement dont s'agit font l'objet de copies ou d'extractions pour communication aux Autorités saisies d'un litige ou aux Auxiliaires de justice, elles devront être chiffrées sur leur support de réception.

Elle 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 la durée de conservation

Le responsable de traitement indique que les informations sont conservées « *10 ans après la rupture de la relation client* » à l'exception des données biométriques et des enregistrements vocaux qui sont conservés « *1 an après rupture de la relation client* ».

Aussi, la Commission rappelle que, conformément à l'article 10-1 de la loi n° 1.165 du 23 décembre 1993, modifiée, « *les informations nominatives doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées (…)* ».

A cet égard, elle observe que le traitement dont s'agit a pour finalité l'authentification de l'identité des clients et de leurs représentants par un dispositif biométrique de reconnaissance vocale.

Ainsi, et tirant toutes conséquences de ses remarques et constatations, la Commission fixe donc la durée de conservation des informations ainsi que suit :

- 3 mois à compter de leur collecte s'agissant des données temporelles ;
- suppression des échantillons de voix ayant servi à l'enrôlement et ceux servant à l'authentification dès après respectivement la réalisation des opérations de création du modèle ou des opérations de comparaison ;
- la durée de souscription au service pour le client ou le temps nécessaire au paramétrage de l'outil concernant les employés volontaires s'agissant du gabarit de l'empreinte vocale ;
- 5 ans après la fin de souscription au service s'agissant des autres informations.

Enfin, elle rappelle que dans le cadre de l'ouverture d'une procédure judiciaire, toute information nécessaire issue du traitement pourra être conservée jusqu'à la fin de la procédure.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement comme suit : « *Authentification de l'identité des clients et de leurs représentants par un dispositif biométrique de reconnaissance vocale* ».

Rappelle que :

- 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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort ;

- si des informations du traitement dont s'agit font l'objet de copies ou d'extractions pour communication aux Autorités saisies d'un litige ou aux Auxiliaires de justice, elles devront être chiffrées sur leur support de réception.

Demande que :

- les traitements relatifs à la gestion des accès et des habilitations et à la gestion des services de téléphonie fixe et/ou mobile sur le lieu de travail, lui soient soumis dans les plus brefs délais ;

- que le responsable de traitement s'assure de l'information préalable de l'ensemble des personnes concernées et qu'elle soit conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Fixe la durée de conservation des informations ainsi que suit :

- 3 mois à compter de leur collecte s'agissant des données temporelles ;
- suppression des échantillons de voix ayant servi à l'enrôlement et ceux servant à l'authentification dès après respectivement la réalisation des opérations de création du modèle ou des opérations de comparaison ;
- la durée de souscription au service pour le client ou le temps nécessaire au paramétrage de l'outil concernant les employés volontaires s'agissant du gabarit de l'empreinte vocale ;
- 5 ans après la fin de souscription au service s'agissant des autres informations.

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 Barclays Bank PLC (Succursale de Monaco), du traitement automatisé d'informations nominatives ayant pour finalité « *Authentification de l'identité des clients et de leurs représentants par un dispositif biométrique de reconnaissance vocale* ».**

Le Président

Guy MAGNAN