Délibération n° 2024-217 du 13 novembre 2024

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

« *Détecter les paiements sortants pouvant présenter un caractère frauduleux et lutter contre la fraude* »

dénommé « *FML* »

présenté par Barclays Bank PLC

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° 1.338 du 7 septembre 2007 sur les activités financières ;

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° 1.284 du 10 septembre 2007 fixant les modalités d'application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, 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'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 déposée par Barclays Bank PLC le 5 aout 2024 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Détecter les paiements sortants pouvant présenter un caractère frauduleux et lutter contre la fraude* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 3 octobre 2024 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 13 novembre 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

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

Afin de lutter contre la fraude, le responsable de traitement souhaite mettre en place un outil lui permettant de détecter les tentatives de fraude par vérification de tous les paiements effectués depuis des comptes des clients de la Banque.

Le responsable de traitement indique que le traitement, objet de la présente demande, porte sur des soupçons d'activités illicites, des infractions, des mesures de sûreté et qu'il est mis en œuvre à des fins de surveillance.

Il est donc soumis au régime de l'autorisation de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Détecter les paiements sortants pouvant présenter un caractère frauduleux et lutter contre la fraude ».*

Il est dénommé « *FML* ».

Les personnes concernées sont les clients et les bénéficiaires de paiements.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

- Maintien d'une liste grise d'IBAN alimentée et mise à jour de manière continue par les équipes Fraud Analytics Barclays situées à Monaco et Londres (dès qu'une fraude est identifiée l'IBAN est rajouté manuellement à la liste enregistrée sur la plateforme) ;

- Analyse des transferts sortants sur la plateforme FML afin de comparer l'IBAN de destination à la liste grise ;

- En cas de « *hit* », génération d'une alerte à l'équipe en charge de lutter contre la fraude à Monaco.

Il est précisé que le paiement n'est pas automatiquement rejeté, *« Une analyse/action manuelle de l'équipe BCG Monaco est effectuée, notamment après avoir pris attache avec le client initiateur du transfert ».* Après cette vérification, il est soit procédé au paiement, soit le paiement est rejeté, le client étant prévenu et pouvant, s'il le désire, porter plainte aux Autorités compétentes. Il est indiqué que la banque se réserve également la possibilité de déposer plainte ou d'effectuer une déclaration de soupçon à l'AMSF.

La Commission rappelle que le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993, mais relève que le processus emporte nécessairement une validation humaine.

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 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement est fondé par la réalisation d'un intérêt légitime.

A cet égard, il expose que *« L'objectif du traitement est de permettre la détection de paiements sortants (i.e des clients de BB PLC Monaco vers des tiers) susceptibles de présenter des anomalies ou un caractère suspect pouvant engendrer des risques de fraude. »*

La Commission relève par ailleurs qu'aux termes de l'Arrêté 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, notamment en son article 94, le responsable de traitement est tenu de se doter d'un *« système d'analyse et de mesure des risques en les adaptant à la nature et au volume de leurs opérations afin d'appréhender »* le risque opérationnel dont fait partie le risque de fraude conformément à l'article 10 du même texte.

La Commission considère 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 nominatives traitées

Les informations nominatives traitées sont :

- Alerte de concordance : IBAN du bénéficiaire du paiement ;

Les informations ont pour origine l'instruction de paiement sortant reçue par le client, lorsqu'elle est exécutée sur les systèmes de la banque.

Le responsable de traitement indique que l'IBAN est la seule donnée utilisée dans le présent traitement, la solution mettant en exergue des opérations qui sont opérées vers des IBANs préalablement portés sur une liste grise. La Commission constate toutefois que les alertes sont relatives à des opérations pour lesquelles d'autres informations sont traitées (nom, prénom, banque destinataire, montants, heure de l'opération etc.). Les informations s'y rapportant relèvent du traitement ayant pour finalité « *Gestion de la clientèle* » et pourront être utilisées, si le responsable de traitement décide de donner des suites légales à la tentative de fraude, au sein du traitement ayant pour finalité « *Dépistage d'opérations illégales* ». Par ailleurs, les modalités de constitutions de la liste grise au sein du groupe ne sont pas précisées, il n'est ainsi pas indiqué si cela repose sur des algorithmes analysant des scénarios prédéfinis. Le cas échéant, la Commission rappelle que le traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165.

La Commission considère ainsi 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***

L'information préalable des personnes concernées est effectuée par le biais d'un document spécifique.

Ce dernier n'étant pas joint, la Commission rappelle que la mention doit être conforme aux dispositions de l'article 14 de la Loi n°1.165 du 23 décembre 1993, modifiée, afin que les personnes concernées soient valablement informées de leurs droits.

- ***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 auprès de la Direction Générale Barclays Bank PLC Monaco par voie postale ou par courrier électronique.

Elle rappelle en outre, que dans le cadre de l'exercice du droit d'accès par voie électronique une procédure doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agit effectivement de 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 cette condition, la Commission 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, modifiée.

V. Sur les destinataires et les personnes ayant accès au traitement

- ***Sur les accès au traitement***

Le responsable de traitement indique que les personnes ayant accès aux informations sont :

- Fraud Analytics (UK/Monaco) : accès à l'outil afin d'enrichir, mettre à jour et potentiellement supprimer des règles de détection des alertes fraudes ;
- Run the Bank (Support) (UK) : maintenance de la plateforme ;
- Banking and Payment Operations (Isle of Man) : lecture seule à des fins de reporting.

Concernant les reportings, la Commission estime qu'il s'agit de données statistiques non nominatives, afin de ne pas étendre le champ des personnes ayant accès/destinataires aux/des informations objets du présent traitement.

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

La Commission rappelle par ailleurs 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.

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

La Commission estime que les informations sont susceptibles d'être communiquées aux Autorités Administratives et Judiciaires légalement habilitées et rappelle que celles-ci ne peuvent avoir communication des informations objet du présent traitement que dans le strict cadre de leurs missions légalement conférées.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d''interconnexions avec les traitements légalement mis en œuvre suivants :

- Gestion et contrôle des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information, aux fins de « *collecte des logs de connexion et des informations temporelles des utilisateurs de la plateforme FML* » ;
- Tenue des comptes de la clientèle afin d'analyser les instructions de paiements sortants des clients de la banque.

Il est également rapproché avec le traitement légalement mis en œuvre ayant pour finalité le « *Dépistage d'opérations illégales* » car « *en cas de fraude avérée, la Banque se réserve le droit/la possibilité de porter plainte et/ou effectuer une déclaration de soupçon auprès de l'AMSF* ».

Il appert également à l'analyse du dossier, que ledit traitement est rapproché avec celui ayant pour finalité la « *Gestion et Supervision de la messagerie professionnelle à des fins de Surveillance* » afin notamment de traiter les alertes.

Ces interconnexions et rapprochements sont conformes 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.

En outre, il convient de rappeler que les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

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 alertes de concordance sont conservées 13 mois. La Commission rappelle toutefois que les informations relatives à l'opération, dont le nom/prénom des bénéficiaires détenteurs d'un IBAN litigieux, devront être conservées selon les durées prévues au sein des traitements concernés.

En ce qui concerne la liste grise d'IBAN, le responsable de traitement indique « *que les durées de rétention n'étaient pas encore définies* ». La Commission rappelle que les IBANs concernés ne peuvent être conservés de manière indéfinie et appelle le responsable de traitement à fixer des modalités de sortie de ladite liste. *A minima*, la Commission estime qu'une transaction ayant été approuvée sur un IBAN porté sur une liste grise devrait conduire à l'en sortir.

Sous ces réserves, la Commission considère que cette durée est conforme aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- le traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 si l'insertion au sein de la liste grise repose sur des scénarios algorithmiques ;

- les documents d'information préalable des personnes concernées doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 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 doit lui être communiquée à première réquisition ;

- dans le cadre de l'exercice du droit d'accès par voie électronique une procédure doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agit effectivement de la personne concernée par les informations ;

- 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 ;

- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises ;

- les IBANs concernés ne peuvent être conservés de manière indéfinie et qu'*a minima*, une transaction ayant été approuvée sur un IBAN porté sur une liste grise devrait conduire à l'en sortir.

Estime que les reportings ne contiennent que des données statistiques non nominatives.

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 Barclays Bank PLC du traitement automatisé d'informations nominatives ayant pour finalité « *Détecter les paiements sortants pouvant présenter un caractère frauduleux et lutter contre la fraude* ».**

Le Président

Robert CHANAS