Délibération n° 2023-106 du 19 juillet 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

« *Détection et analyse des fraudes sur paiements sortants* »,

présenté par Banque J. Safra Sarasin (Monaco) SA

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 du 28 janvier 1981, 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 la Banque J. Safra Sarasin (Monaco) SA, le 31 mars 2023, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Détection et analyse des fraudes sur paiements sortants* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 31 mai 2023, conformément à l'article 11-1 de la Loi n° 1.165, susmentionnée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 19 juillet 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Banque J. Safra Sarasin (Monaco) SA est enregistrée au RCI sous le numéro 89S0255 ayant pour activité la réalisation de « *toutes opérations de banque pour elle-même, pour le compte de tiers ou en participation et notamment sans que cette énumération soit limitative, des opérations financières, de crédit, d'escompte, de bourse ou de change de gestion de patrimoine, ainsi que toutes opérations annexes ou connexes et celles généralement quelconques nécessaires à la réalisation de l'objet social* ».

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 « *Détection et analyse des fraudes sur paiements sortants* ».

Les personnes concernées sont les clients (personnes physiques, personnes morales, mandataires, bénéficiaires économiques), les tiers et les gérants externes.

Les fonctionnalités du traitement sont les suivantes :

- établissement de modèles de risques se basant notamment sur l'analyse du comportement habituel du client (heure ou jour inhabituel, montant, etc.) ;
- analyse de tous les paiements sortants, en temps réel, afin de détecter des tentatives de fraudes présumées en se basant sur des algorithmes (attribution d'un score de risque) et un profilage dynamique ;
- gestion des alertes et analyse de premier niveau par une équipe spécialement dédiée pour écarter les faux positifs ;
- en cas de suspicion de fraude confirmée, communication par email de l'alerte au Service Compliance pour investigation (déblocage de l'opération ou rejet) ;
- établissement d'une liste d'IBAN tiers à la Banque suspects.

Le responsable de traitement précise que l'outil analyse l'ensemble des paiements sortants (des comptes clients vers l'extérieur de la Banque) en opérant une comparaison avec l'historique des transactions du client et/ou les modèles de fraude déjà rencontrés pour le destinataire des fonds sortants. Dans l'hypothèse où le score de risque est en dessous du plafond, la transaction sera débloquée. Dans le cas contraire, la transaction est immobilisée pour analyse complémentaire.

A ce sujet, le responsable de traitement poursuit en indiquant qu'une équipe disposant de « *l'expérience et la connaissance pour filtrer les « faux positifs » des « vrais positifs »* » a été mise en place afin de procéder à l'analyse complémentaire de l'alerte lorsque la transaction a un score de risque supérieur au plafond prédéfini. Si après analyse la transaction apparait toujours comme suspecte, cette équipe transmet l'alerte, par email, au Service Compliance afin que ce dernier procède à une investigation plus approfondie, pouvant aller jusqu'à la vérification de l'opération auprès du client.

La Commission constate par ailleurs que le présent traitement d'informations nominatives permet au responsable de traitement de constituer une *« base composée d'IBAN* » qu'il qualifie de *« nomenclature d'IBAN réservés »*. Le responsable de traitement poursuit en indiquant qu'intégreront cette base les IBAN appartenant à des *« tiers liés à une tentative/réalisation de soustraction frauduleuse* ».

A cet égard, la Commission rappelle que le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 et estime qu'une transaction signalée comme suspecte par l'outil en raison de l'apparition de son bénéficiaire dans la « *nomenclature d'IBAN réservés* », doit en tout état de cause faire l'objet d'une analyse par l'équipe spécialement dédiée et ne doit pas conduire à un blocage automatique de l'opération sans aucune intervention humaine.

Elle prend acte des précisions apportées par le responsable de traitement selon lesquelles *« le placement sur la nomenclature d'IBAN réservés est automatiquement réversible – il suffit que l'IBAN aboutisse à un dénouement non contesté pour qu'il soit automatiquement retiré de la base »*.

La Commission constate enfin que le traitement permet également la constitution de preuves en cas de litige.

Sous la réserve évoquée au présent point, la Commission considère 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 présent traitement est justifié par la réalisation d'un intérêt légitime que le responsable de traitement poursuit, et ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

A cet égard, le responsable de traitement indique qu'il souhaite *« se doter d'une technologie plus performante permettant un contrôle complémentaire des paiements sortants et ainsi protéger le client en évitant la fraude et l'usurpation d'identité ».*

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 traitées

Les informations nominatives traitées sont :

- données relatives à l'identité du client : identifiant unique du compte, type de compte, code interne de la banque, identifiant unique du client titulaire du compte, type de client titulaire du compte contrat numérique bancaire / login ID, ratio du solde du compte pré-transactionnel, indicateurs de risque du compte, indicateur de risque du client ;
- données relatives au paiement : identifiant unique de l'ordre, identifiant unique du paiement, type de saisie d'ordre, méthode de paiement, type de paiement, date de valeur du paiement, montant, montant converti, devise de la transaction, devise locale, horodatage de la création du paiement ; score de risque attribué par l'outil ;
- données relatives à l'identité du bénéficiaire : nom complet, identifiant unique de sa banque, pays de la banque, adresse du bénéficiaire, pays du bénéficiaire ;
- données relatives à l'utilisateur : identifiant, typologie d'utilisateur, fonction, département, branche ;
- données d'identification électronique : user ID ;
- informations temporelles : Payment Creation Timestamp ;
- alertes : saisie d'écran de l'alerte, faux positifs.

La Commission constate que sont également exploités les logs de connexion des personnes habilitées.

Par ailleurs, le responsable de traitement indique que les informations transactionnelles sont communiquées à l'outil par le logiciel en charge de la gestion des comptes clients au sein de la banque.

Enfin, les données d'identification électronique ainsi que les informations temporelles ont pour origine le système de la banque.

La Commission considère 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, modifiée.

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 mention ou clause particulière intégrée dans un document remis à l'intéressé ;
- d'une rubrique propre à la protection des données accessible en ligne ;
- d'une mention particulière intégrée dans un document d'ordre général accessible en ligne.

La Commission n'ayant pas été destinataire desdits documents, elle n'est pas en mesure de se prononcer sur la qualité de l'information dispensée.

Aussi elle rappelle que l'ensemble des personnes concernées doit être informé conformément aux dispositions de 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 par voie postale auprès du Service Compliance.

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

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 qu'ont accès au traitement :

- Central Fraud Prevention Team (département localisé dans la branche Suisse du Groupe spécialisé dans le monitoring des opérations de paiements et de détection de la fraude) : en consultation et mise à jour ;
- administrateurs IT habilités du Groupe : en consultation, mise à jour et inscription dans le cadre de leurs travaux de maintenance mais n'ont pas accès au serveur physique ;
- utilisateurs : les membres du Service Compliance en inscription, modification, mise à jour et consultation ;
- membres du Service Contrôle Permanent : en consultation uniquement *a posteriori*.

La Commission considère que ces accès sont conformes aux exigences légales et sont justifiés au regard de la finalité du traitement.

➢ ***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 avec d'autres traitements

Le responsable de traitement indique que le présent traitement est interconnecté avec les traitements, légalement mis en œuvre :

- « *Détection et analyse des transactions réalisés par des clients qui pourraient être liées au blanchiment de capitaux, au financement du terrorisme et à la corruption* » ;
- « *Tenue des comptes de la clientèle et des informations s'y rattachant par les établissements bancaires et assimilés* ».

A l'étude du dossier, la Commission relève que le présent traitement est rapproché/interconnecté avec les traitements, légalement mis en œuvre suivants :

- « *Gestion administrative des salariés* » ;
- « *Gestion de la messagerie électronique professionnelle à des fins de surveillance et de contrôle* » ;
- « *Gestion du contentieux* ».

La Commission considère que ces interconnexions et ces 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.

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 données relatives au score de risque sont purgées après *« une période glissante de 18 mois »*.

Par ailleurs, le responsable de traitement indique que les logs des opérations *« ont pour vocation d'être conservés pour une durée n'excédant pas dix-huit (18) mois »*.

Les logs de connexion sont conservés quant à eux un an.

Les informations des IBAN classifiés réservés sont conservées comme indiqué au point I de la présente délibération.

Enfin, le responsable de traitement a précisé que la durée de conservation des informations liées aux opérations est de *« cinq années à compter de la date d'émission de la donnée acquise par l'application »*.

La Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 ;

- les IBAN tiers classifiés comme réservés doivent en tout état de cause faire l'objet d'une analyse par opération par l'équipe spécialement dédiée ;

- l'information de l'ensemble des personnes concernées soit préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- 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.

Sous le bénéfice de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre, par la Banque J. Safra Sarasin, du traitement automatisé d'informations nominatives ayant pour finalité *« Détection et analyses des fraudes sur paiements sortants ».***

Le Président

Guy MAGNAN