Commission Nationale de l'Informatique et des Libertés

Délibération n° 2016-037 du 18 février 2016

autorisant La Banque Postale à mettre en œuvre

un système d'authentification des titulaires de cartes bancaires

par reconnaissance vocale.

(Demande d'autorisation n° 1842385)

La Commission nationale de l'informatique et des libertés,

Saisie par La Banque Postale d'une demande d'autorisation concernant un traitement automatisé de données à caractère personnel ayant pour finalité la mise en œuvre d'un système d'authentification des porteurs de cartes bancaires par reconnaissance vocale ;

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 ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, notamment son article 87 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 25-I-8° ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu les délibérations n° 2013-198 du 11 juillet 2013 et n° 2014-306 autorisant la Banque Postale à mettre en œuvre à titre expérimental un système d'authentification des titulaires de carte bancaire avec pour biométrie utilisée, la reconnaissance vocale (Talk To Pay) pour une durée totale de deux ans ;

Après avoir entendu M. François Pellegrini, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La Commission nationale de l'informatique et des libertés a autorisé, par délibération n° 2013-198 du 11 juillet 2013, La Banque Postale à mettre en œuvre à titre expérimental un système d'authentification de titulaires de cartes bancaires par reconnaissance vocale, pour une durée d'un an. Au regard des premiers résultats positifs exposés dans le bilan adressé à la Commission, La Banque Postale a été autorisée, par délibération n° 2014-306 du 10 juillet 2014, à proroger l'expérimentation d'une durée d'un an. Le bilan adressé à l'issue de cette deuxième phase d'expérimentation confirme les résultats obtenus en juillet 2014, quant à l'appétence des six cent vingt utilisateurs pour le service proposé (fluidité des parcours, sentiment de sécurité) dont le taux de satisfaction s'est élevé à 86 % et quant aux apports du dispositif de reconnaissance vocale.

La Commission observe que la mise en place d'une authentification forte des clients souhaitant régler des transactions en ligne répond à un phénomène de fraude aux paiements à distance en constante augmentation. L'authentification forte repose sur l'utilisation de plusieurs éléments d'authentification se répartissant en trois catégories : ce que la personne connaît (par exemple un mot de passe), ce que la personne possède (par exemple son téléphone), ce que la personne est (par exemple, la reconnaissance d'une caractéristique biométrique). Une condition d'efficacité de l'authentification forte est qu'elle soit largement adoptée par les personnes concernées. Cette adoption dépend du caractère universel des facteurs d'authentification choisis et des contraintes d'utilisation afférentes

liées, par exemple, aux difficultés de mémoriser un mot de passe ou de porter en permanence sur soi un objet.

C'est dans ce contexte et pour répondre aux dispositions de la directive du 25 novembre 2015 concernant les services de paiement dans le marché intérieur que La Banque Postale souhaite généraliser le système d'authentification par reconnaissance vocale expérimenté pendant deux ans, afin de renforcer les mécanismes d'authentification préalable des utilisateurs de la solution de paiement LBP Pay.

Contrairement au protocole 3D Secure, dont la mise en place est à la main des sites de commerce en ligne, la reconnaissance vocale serait utilisée pour accéder à une solution de paiement appelée LBP Pay proposée directement par la banque émettrice de la carte bancaire utilisée. Cette solution de paiement ne nécessite pas d'intégration par le site de commerce en ligne et s'affiche automatiquement lorsque la personne concernée arrive sur le formulaire permettant de saisir les numéros de sa carte bancaire.

Intégrée au portefeuille de service Mes Paiements , elle permet de générer un cryptogramme dynamique à usage unique à trois chiffres afin de sécuriser les données de carte bancaire communiquées et lutter contre l'hameçonnage (phishing) des données ou l'utilisation frauduleuse des numéros de cartes.

La solution LBP Pay est accessible aux clients de La Banque Postale, soit depuis leur espace client sur le site de la banque en ligne, soit au travers d'une application dédiée aux paiements fournie par La Banque Postale.

La Commission observe que le projet de traitement automatisé prévoit le recours à des données biométriques pour assurer le contrôle de l'identité des personnes. Il relève, à ce titre, du 8° du I de l'article 25 de la loi du 6 janvier 1978 modifiée et doit dès lors être autorisé par la CNIL.

Sur la finalité du traitement :

La méthode d'authentification choisie fait appel à deux facteurs, à savoir la réception d'un appel sur le téléphone préalablement enrôlé de la personne concernée et la reconnaissance de la voix afin d'identifier cette dernière. La reconnaissance vocale intervient dans le processus d'authentification classiquement utilisé dans le cadre du protocole 3D Secure, à savoir la possession du téléphone réceptionnant un message texte comportant le code permettant de déclencher le paiement.

La Banque Postale souhaite par ce biais simplifier le parcours d'authentification du client en proposant, en tant qu'alternative à la saisie d'un code à usage unique, un appel sortant sur le téléphone mobile préalablement enrôlé, couplé à la reconnaissance de la voix de la personne concernée.

L'activation de la solution LBP Pay par authentification vocale est précédée d'un processus en quatre étapes permettant de s'assurer de l'identité du titulaire de la carte bancaire préenregistrée.

En premier lieu, la personne concernée doit activer le service de sécurisation d'opérations sensibles Certicode en s'adressant à un conseiller dans son bureau de poste gestionnaire de compte courant, lequel vérifie l'identité du client et le fait qu'il est titulaire de la ligne à contacter lors de l'activation de la solution de paiement.

En deuxième lieu, la personne concernée doit activer le portefeuille de services Mes Paiements , soit en se rendant sur son espace client en ligne, soit en utilisant l'application de La Banque Postale Mes Paiements , après s'être authentifiée par la saisie d'un identifiant et mot de passe. Elle doit ensuite saisir dans l'espace prévu à cet effet le code de validation à usage unique reçu par message texte sur son numéro de téléphone mobile validé par l'intermédiaire de la procédure Certicode.

En troisième lieu, la saisie du code permet d'activer le service de paiement, et d'enregistrer les numéros de cartes bancaires rattachées au compte du titulaire, après saisie du cryptogramme correspondant.

En quatrième lieu, la personne concernée reçoit un courrier postal comportant le code d'activation de la solution de paiement à saisir sur son espace client banque en ligne, ainsi qu'un identifiant à huit chiffres nécessaire pour installer la solution de paiement LBP Pay, sous forme d'extension de navigateur internet, sur son terminal. L'extension LBP Pay est une application installée sur le navigateur internet s'affichant automatiquement sur les formulaires de paiement en ligne et permettant de procéder au pré-remplissage automatique desdits formulaires après avoir authentifié le client. Le cryptogramme dynamique à usage unique est généré à cette occasion.

Lors de la première utilisation de l'extension LBP Pay, le client saisit l'identifiant à huit chiffres communiqué par courrier postal et choisit le mode d'authentification permettant de déclencher le paiement. Trois options lui sont alors offertes entre l'authentification vocale, la saisie d'un code à usage unique envoyé par message texte (3DS) ou encore l'authentification par le biais d'une application préalablement téléchargée sur son ordiphone et enrôlée. S'il choisit la reconnaissance vocale, le client est appelé sur son téléphone mobile pour s'enrôler ; il est alors invité à prononcer les phrases dictées par des consignes vocales afin de créer un modèle vocal. Lors des authentifications suivantes, le client est de nouveau appelé et invité à répéter une phrase d'authentification, qui sera comparée au modèle vocal constitué lors de son enrôlement.

La reconnaissance du locuteur se base sur la modélisation physique des caractéristiques du conduit vocal de la personne concernée. Un modèle de voix est créé en enrôlant des échantillons vocaux de la personne. Le système détermine si c'est bien le locuteur qui parle ou non dans l'enregistrement.

Une des propriétés du modèle vocal constitué lors de l'enrôlement est qu'il est non réversible ; les traits biométriques - ici la voix de l'utilisateur - ne peuvent pas être reconstitués à partir du modèle. En effet, ce modèle représente une distribution de probabilités d'un certain nombre de caractéristiques de la voix et n'est pas un enregistrement de celle-ci.

Sur le fondement juridique du traitement :

Le traitement de reconnaissance vocale repose, conformément à l'article 7 de la loi du 6 janvier 1978, sur le consentement spécifique, libre et éclairé de la personne concernée, qui choisit de recourir à ce mode d'authentification lors de l'utilisation de l'extension LBP Pay. La solution offre des dispositifs d'authentification alternatifs à la reconnaissance vocale, sans surcoût ni contrainte particulière pour la personne concernée.

Il est possible de revenir à tout moment et sans frais sur les choix exprimés quant au mode d'authentification et d'obtenir la suppression des modèles biométriques constitués lorsque la personne concernée signifie qu'elle ne souhaite plus utiliser l'authentification vocale.

Sur la nature des données traitées :

Les données collectées auprès des clients choisissant de recourir à l'authentification vocale sont les suivantes :

- nom, prénom ;
- numéro de la carte bancaire que la personne concernée choisit d'enregistrer dans l'outil ;
- numéro de téléphone mobile, adresse électronique ;
- modèle biométrique vocal (l'enregistrement permettant de produire le modèle biométrique vocal n'est pas conservé).

La Commission considère que la collecte de ces données est proportionnée à la finalité poursuivie.

Sur la durée de conservation des données :

Les nom, prénom, numéro de carte bancaire, numéro de téléphone mobile, adresse électronique, ainsi que le modèle biométrique vocal sont stockés pour la durée de souscription au service avec la méthode d'authentification biométrique.

Les demandes d'authentification sont tracées et conservées pendant quinze mois.

Sur les destinataires des données :

Seul aura accès aux données le personnel spécifiquement habilité à cet effet de la Banque Postale ainsi que de son prestataire sous-traitant, soumis à des obligations de confidentialité renforcées.

Sur l'information et les droits des personnes :

Les personnes concernées sont informées de leurs droit d'accès, de rectification et d'opposition par des mentions d'information figurant sur les formulaires de souscription au service, par les mentions légales figurant sur le site de la Banque en ligne, et par l'envoi d'un courrier spécifique.

Les personnes concernées peuvent demander à tout moment et sans frais la suppression de leur modèle vocal biométrique si elles ne souhaitent plus utiliser ce mode d'authentification.

Sur la sécurité des données et la traçabilité des actions :

A l'issue de l'expérimentation, La Banque Postale a réalisé une étude d'impact du traitement sur la vie privée des personnes concernées. Les mesures techniques adoptées ont permis de réduire à un niveau de vraisemblance et de gravité faible les impacts résultant notamment des risques de fuites ou de pertes des données, d'indisponibilité du dispositif ou d'usurpation d'identité.

Toutes les communications web sont sécurisées au moyen du protocole HTTPS. Concernant le recours à ce protocole, la Commission recommande d'utiliser la version de TLS la plus à jour possible.

Les modèles biométriques sont conservés sous forme chiffrée dans une bulle monétique chez un sous-traitant de La Banque Postale, et sont isolés des données d'identité des personnes concernées.

Les serveurs hébergeant les modèles biométriques sont protégés par des mesures physiques (caméras de vidéosurveillance sur le site d'hébergement, contrôle d'accès par badge au locaux sécurisés hébergeant les serveurs) et logiques (système de détection d'intrusion, confinement du traitement dans un des réseaux isolés des autres traitements).

Une journalisation des opérations de consultation, création et modification du traitement est réalisée.

Le personnel habilité par La Banque Postale accédera aux données au moyen d'une authentification forte (token RSA).

En cas de défaillance ou de mauvais fonctionnement du système d'authentification par reconnaissance vocale, la personne concernée peut renouveler son enrôlement pour l'optimiser.

En tout état de cause, le modèle biométrique est mis à jour à chaque fois que l'utilisateur a été fermement reconnu par le dispositif de reconnaissance vocale, de manière à intégrer sur le long terme les variations de la voix d'un locuteur.

La Commission prend note que La Banque Postale s'engage, dans un délai ne pouvant excéder douze mois, à ne conserver les gabarits biométriques que sous forme chiffrée et à ce que les clés de chiffrements/déchiffrement soient uniquement détenues par les utilisateurs. A l'issue de ce délai, lors d'une phase authentification, un dispositif à la main de l'utilisateur (extension navigateur ou application ordiphone) enverra la clé de déchiffrement

du gabarit au serveur, qui ne pourra la conserver que le temps de procéder à l'authentification de l'utilisateur et éventuellement de mettre à jour le gabarit dans le cas d'une authentification réussie.

Par ailleurs, la Commission observe que ce dispositif d'authentification ne dispose pas de mécanisme contre le re-jeu, ce qui permet à un attaquant qui disposerait du téléphone du client et aurait enregistré une phrase d'authentification, de la rejouer afin d'usurper l'identité dudit client. La Commission note qu'une partie de la phrase prononcée par l'utilisateur pour s'authentifier est susceptible d'être répétée fréquemment dans différents contextes et d'être prononcée sur la messagerie vocale. La Commission recommande que La Banque Postale déploie un mécanisme anti-rejeu et choisisse une phrase d'authentification moins fréquemment prononcée.

La Commission prend acte que le dispositif biométrique proposé ne saurait à lui seul représenter un moyen d'authentification fiable. Ce dispositif biométrique n'a pas vocation à fournir un moyen d'authentification autonome mais vient renforcer un dispositif existant s'appuyant sur la possession d'un objet.

Dans ces conditions, **la Commission autorise** La Banque Postale à mettre en œuvre un système d'authentification des titulaires de cartes bancaires par reconnaissance vocale.

La Présidente
Isabelle FALQUE-PIERROTIN
