Swiss Banking

Gestion des données dans les activités bancaires courantes

Mai 2021

Guide de l'ASB

	Executive Summary	3
1	Introduction	4
2	Concepts normatifs généraux en matière de traitement des données	6
	2.1 Bases nécessaires pour une bonne gestion des données	6
	2.2 Profilage	9
	2.3 Motifs justificatifs	9
	2.4 Mesures techniques et organisationnelles (MTO)	11
	2.5 Gouvernance de l'IA	13
3	Cas concrets	16
	3.1 Recours à l'intelligence artificielle à des fins de compliance	16
	3.2 Examen de crédit	18
	3.3 Analyses de tendance et benchmarking	20
	3.4 Authentification biométrique	22
	3.5 Offres et conseils personnalisés	24
	3.6 Programmes de fidélité	27

Executive Summary

Le présent guide expose des concepts normatifs généraux en matière de traitement de données, en se référant à six cas concrets représentatifs des activités bancaires. Il met l'accent sur les éléments fondamentaux de la nouvelle loi sur la protection des données (nLPD), la gestion des motifs justificatifs, les mesures techniques et organisationnelles (MTO) ainsi que le recours à l'intelligence artificielle (IA), en particulier dans le cadre du traitement automatisé de données personnelles. Ce guide s'adresse au premier chef aux membres de l'Association suisse des banquiers (ASB) et leur propose des lignes directrices qui leur permettront d'exploiter en toute sécurité les opportunités liées à l'utilisation des données.

- **Recours à l'IA à des fins de compliance:** la banque doit évaluer le risque inhérent à l'utilisation de l'IA puis, idéalement, élaborer un plan opérationnel. Il lui appartient en particulier de documenter des MTO appropriées, qui seront choisies en veillant au respect des principes du droit relatif à la protection des données en matière de traitement de données.
- **Examen de crédit:** les données utilisées devraient être d'une qualité irréprochable et permettre d'identifier clairement leur source à tout moment. Au regard du droit relatif à la protection des données et afin d'assurer une qualité parfaite de toutes les données utilisées, il convient de ne pas traiter de données dont la provenance est douteuse ou qui sont difficiles, voire impossibles à vérifier.
- **Analyses de tendance et benchmarking:** l'anonymisation des données personnelles recèle un risque résiduel de réidentification. Il convient donc de s'assurer, au moyen de MTO appropriées, que toute réidentification est exclue. Il convient également de concevoir les analyses de telle sorte qu'au besoin, la banque pourra fournir des explications claires sur la composition des blocs de données ainsi que sur les méthodes de traitement mises en œuvre.
- **Authentification biométrique:** pour apprécier le caractère approprié des MTO, par exemple en ce qui concerne le stockage de données, il convient de prendre dûment en compte les données biométriques, qui sont des données personnelles sensibles. Une communication transparente quant au recours à des systèmes biométriques de reconnaissance est de nature à abaisser le seuil d'acceptabilité de ces procédés par les clients.
- **Offres et conseils personnalisés:** si les exigences fondamentales sont remplies et en vertu du principe de la bonne foi, l'analyse de données à cette fin est toujours autorisée sans contrainte particulière dès lors qu'elle repose sur des données fournies par le client lui-même et collectées par la banque dans le cadre de son activité bancaire typique.
- **Programmes de fidélité:** la fidélisation standardisée des clients n'est pas problématique au regard de la protection des données. S'agissant en revanche des programmes de fidélité individualisés, les banques sont tenues notamment d'un devoir d'informer. Avant d'être intégré dans un tel programme, le client doit en être averti et recevoir des informations. La banque peut être libérée du devoir d'informer si le client a déjà reçu des informations à l'ouverture de la relation d'affaires.

1 Introduction

L'utilisation des données revêt une importance croissante pour le secteur financier. La manière dont ces données peuvent et doivent être utilisées connaîtra encore de profonds changements ces prochaines années, impulsés par les évolutions technologiques, les nouveaux besoins des clients[1] et les exigences réglementaires. Une utilisation efficace des données permet aux établissements financiers de personnaliser les produits et services proposés, et ainsi de les rendre plus pertinents. Il en résulte en fin de compte une amélioration du conseil à la clientèle. En outre, une utilisation optimale des données se traduit par une efficacité accrue des processus, par des réductions de coûts et par une meilleure gestion des risques. Mais dans le même temps, l'intégrité et la confiance des clients demeurent des priorités absolues pour les banques suisses. Cela impose avant tout de la transparence en ce qui concerne les traitements de données et leur finalité. Il est donc essentiel que le secteur financier, confronté aux problématiques inhérentes à une gestion responsable des données, prenne en compte non seulement les aspects réglementaires et techniques (comme p. ex. la sécurité des données), mais aussi la perspective des clients ainsi que leurs attentes.

C'est dans ce but – et dans le contexte de l'introduction de la nLPD – qu'un groupe de travail placé sous l'égide de l'ASB a élaboré le présent guide. Celuici donne des éclairages sur six cas concrets de traitement de données et vise à aider les banques dans leur gestion courante des données. Il constitue donc un outil destiné au premier chef aux membres de l'ASB. Loin de fixer des principes juridiques ou éthiques, il présente des situations issues de la pratique qui jouent d'ores et déjà un rôle important dans le quotidien bancaire. Il se distingue en cela d'autres publications qui privilégient une approche globale ou fixent des règles de conduite générales à l'échelle sectorielle (code of conduct). Ce guide n'entend pas définir des normes minimales valables pour l'ensemble de la branche. Par ailleurs, il ne prétend pas à l'exhaustivité et, au besoin, il sera mis à jour et complété périodiquement. Chaque établissement financier reste libre d'interpréter et/ou d'appliquer les préconisations formulées dans ce document en fonction de sa propre évaluation des risques.

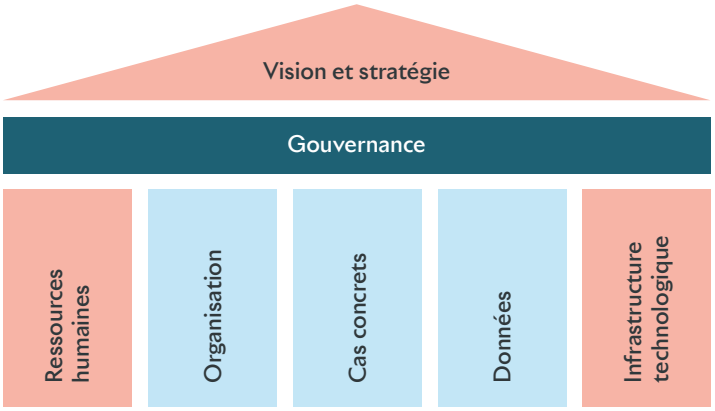
Structure du présent guide

Les facteurs à prendre en compte dans la gestion des données au quotidien sont mis en lumière ci-après à l'aide d'un schéma récapitulatif (voir graphique 1). Outre l'organisation, les données et les cas concrets sur lesquels se focalise le présent guide, d'autres facteurs jouent en effet un rôle essentiel: la vision et la stratégie de l'entreprise, ou encore la gestion des ressources humaines, des aspects culturels et de certains éléments concernant l'infrastructure technologique. Vu toutefois le caractère extrêmement spécifique de ces facteurs, c'est à chaque établissement de s'en emparer à sa propre échelle, de sorte que le présent guide les évoque marginalement, voire pas du tout.

1 Par souci de lisibilité, il est fait usage, dans la présente publication, du masculin générique. Les termes employés s'appliquent donc sans distinction à tous les genres. Ce choix résulte de considérations purement rédactionnelles et n'implique aucun jugement de valeur.

Graphique 1

Schéma récapitulatif des facteurs à prendre en compte dans la gestion des données



Source: ASB

S'agissant du choix des cas concrets abordés, l'objectif prioritaire est de couvrir largement l'activité bancaire. Selon les situations, une utilisation efficace et ciblée des données peut être fructueuse dans le cadre des prestations existantes destinées aux clients, du développement de nouvelles prestations ou de l'atténuation des risques. Les risques[2] inhérents aux cas concrets sont à évaluer selon la nature et le volume des données concernées ainsi que selon la forme de traitement à laquelle celles-ci sont soumises. Il y a lieu de procéder à cette évaluation dans le cadre de la gouvernance interne à la banque et, en termes de politique d'entreprise, de prendre les décisions en résultant dans le respect des principes du droit relatif à la protection des données comme la limitation des finalités, la transparence, la licéité et la proportionnalité (p. ex. sous l'angle de la parcimonie). Des mesures techniques et organisationnelles (MTO) facilitent la mise en œuvre appropriée et efficace des exigences légales (voir chapitre 2.4).

La relation entre la banque et ses clients doit également être prise en compte. A cet égard, les différents moyens d'information des clients peuvent être mis à profit pour favoriser un climat de confiance. De même, il convient d'examiner dans chaque cas concret s'il existe un écart entre les attentes des clients et les activités réelles de la banque. Cet éventuel écart doit être éliminé, le cas échéant au moyen d'une déclaration de confidentialité ou d'autres mesures de transparence. L'organisation concrète de la gouvernance dépend de la taille, de la structure, de la complexité, du modèle d'affaires et des risques de la banque concernée. Pour chacun des cas concrets ci-après, on considère qu'une gouvernance est en place. Les éléments détaillés requis sont structurés comme suit :

a. **Contexte:** introduction au sujet et valeur ajoutée pour les clients et les banques
b. **Applications possibles:** présentation succincte de différents exemples
c. **Problématiques éventuelles:** questions qui se posent et solutions possibles

2 Il peut s'agir en particulier de risques juridiques, de risques de réputation ou de risques opérationnels.

2 Concepts normatifs généraux en matière de traitement des données

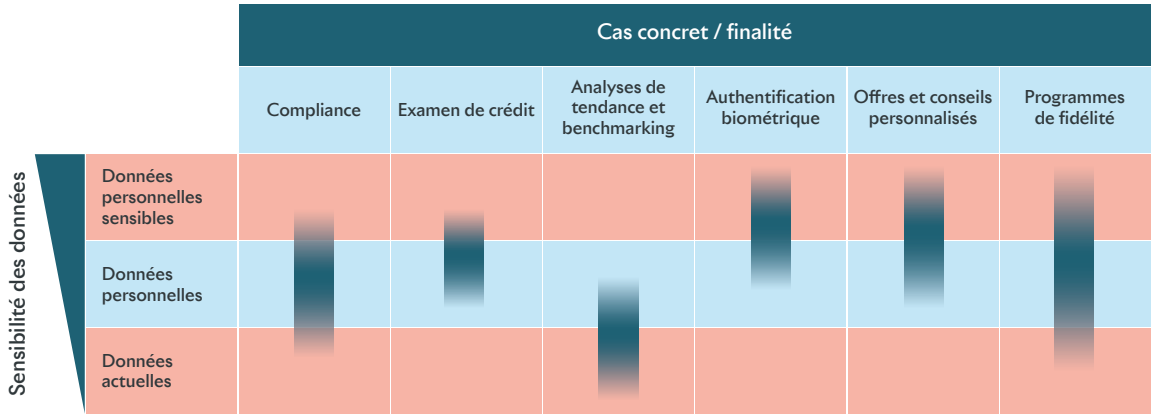
2.1 Bases nécessaires pour une bonne gestion des données

Quelle que soit la nature des données traitées, le contexte de leur utilisation doit toujours être pris en compte. Tant la LPD en vigueur que la nLPD permettent une classification sommaire des données selon les catégories suivantes:

1. **Données factuelles [3] (non expressément mentionnées dans la nLPD):** données qui, faute de lien avec des personnes précises, ne permettent pas d'identifier des individus et ne sont donc pas des données personnelles. Les données anonymisées entrent dans cette catégorie. Logiquement, les données factuelles n'entrent pas dans le champ de la nLPD.
2. **Données personnelles (art. 5, let. a nLPD):** toutes les données qui présentent un lien avec des personnes précises, y compris par exemple en combinaison et en corrélation avec d'autres données. Il peut s'agir de données statiques, mais aussi de données qui permettent de déduire le comportement d'une personne. Exemples: données de transaction ou géodonnées.
3. **Données personnelles sensibles (art. 5, let. c nLPD):** données personnelles figurant dans la liste abstraite et exhaustive définie par le législateur. Exemples: données biométriques, données sur les opinions ou les activités religieuses et philosophiques, mais aussi informations sur la sphère intime ou sur la santé [4].

Graphique 2

Analyse croisée de la finalité du traitement et de la sensibilité des données



Source: ASB

3 Il peut s'agir en particulier de risques juridiques, de risques de réputation ou de risques opérationnels.

4 Voir la liste complète à l'art. 5 nLPD.

Cette répartition des données en trois catégories – données factuelles, données personnelles et données personnelles sensibles – permet de classer schématiquement les cas concrets retenus en fonction de leur sensibilité. Il ressort toutefois du présent guide que, juridiquement, la distinction n'est pas toujours nette.

La sensibilité des données évoquée ci-dessus résulte du droit relatif à la protection des données et ne correspond pas nécessairement à la sensibilité subjective perçue par les clients. Y compris au sein d'une même catégorie de données, il peut être judicieux d'opter pour une approche plus ou moins stricte en fonction de la sensibilité subjective et de la situation de risque correspondante. La gestion des données personnelles des clients des banques, dites Client Identifying Data (CID)[5], est soumise non seulement aux principes du droit relatif à la protection des données, mais aussi au secret professionnel du banquier au sens de l'article 47 de la loi sur les banques (LB)[6], lequel renforce par des sanctions pénales les obligations de confidentialité prévues par le droit civil. Dans ce contexte, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a fixé un certain nombre d'exigences techniques et organisationnelles en ce qui concerne la gestion des données électroniques de clients[7]. La liste des catégories de données figurant sur le graphique 2 n'entend pas être exhaustive, elle se borne à donner un aperçu visuel sommaire des cas concrets examinés au chapitre 3. On a retenu sciemment une définition large de la notion de «sensibilité des données», afin qu'elle soit pertinente en relation avec les risques de réputation, la perception des clients et du public, et enfin les problématiques éthiques. De fait, toute évaluation individuelle des risques effectuée par une banque reflète la propension au risque de cette banque, de sorte qu'elle est susceptible de varier.

Privacy Icons

Tout traitement de données personnelles doit être visible pour la personne concernée. En général, il lui est signalé et expliqué au moyen d'un document spécifique: la déclaration de protection des données ou déclaration de confidentialité. Mais il est rare que ce document soit lu autrement que de manière superficielle – s'il est lu. Afin de rendre les traitements de données plus transparents, on peut utiliser des pictogrammes: l'association Privacy Icons (www.privacy-icons.ch/) en propose gratuitement, à des conditions de licence simples. Diverses entreprises suisses, dans tous les domaines, recourent déjà à cette solution ou à des solutions similaires.

5 La notion de «CID» est une notion développée par la FINMA. Elle englobe les données d'identification des personnes physiques ainsi que des sociétés de domicile, trusts, etc. utilisés par elles. Ces personnes sont appelées «particuliers».

6 Les données de personnes morales et d'autres entreprises, y compris de sociétés de domicile et de trusts, ne sont plus considérées comme des données personnelles au sens de la nLPD dès lors qu'elles ne présentent pas de lien avec une personne physique. Toutefois, les données de personnes morales (et de clients institutionnels) sont couvertes par le secret professionnel du banquier.

7 Voir en particulier la Circ.-FINMA 2008/21 «Risques opérationnels – banques», annexe 3, «Traitement des données électroniques de clients».

A propos de… l'open banking et l'open finance

A l'heure où la fragmentation de la chaîne de création de valeur va croissant, les prestataires de services financiers qui interviennent auprès des clients – banques, entreprises d'assurance, entreprises Fintech, non-banques – sont de plus en plus diversifiés. L'ASB a examiné ces évolutions en détail dans un état des lieux consacré à l'open banking et l'open finance. Quant au présent guide, il se focalise sur les échanges de données (de clients) résultant de ces interactions entre banques et prestataires externes.

Les applications potentielles de l'open banking et l'open finance sont nombreuses, tant dans le segment de la clientèle Entreprises que dans celui des particuliers. Les exemples ci-après illustrent quelques-unes de ces applications:

- **planification des liquidités:** meilleure visibilité pour la clientèle Entreprises grâce à l'intégration des logiciels de comptabilité
- **agrégation de la situation financière:** pour la clientèle Entreprises comme pour les particuliers, transparence accrue grâce à l'agrégation de plusieurs comptes et de diverses valeurs patrimoniales via un prestataire tiers
- **paiements:** transactions plus simples, plus rapides et plus sûres par le biais d'un prestataire externe

Toutes ces applications potentielles ont en commun de générer des flux de données de clients entre les banques et les prestataires tiers. Dans ce cadre, les banques sont tenues de respecter les exigences du droit relatif à la protection des données et du secret professionnel du banquier. Du point de vue des clients, la question est de savoir à quelles conditions une banque est autorisée à communiquer des données personnelles à des prestataires tiers. Selon la nature et l'intensité de la coopération entre la banque et ces prestataires tiers, les obligations de contrôle et de diligence de la première envers les seconds sont plus ou moins strictes.

La coopération et les flux de données entre le client, la banque et les prestataires tiers doivent être documentés clairement, le cas échéant par contrat, sans oublier la possibilité que deux banques (ou davantage) pratiquent entre elles l'open banking et l'open finance. Enfin, la transparence envers le client joue un rôle décisif. Il y a donc lieu de lui faire savoir quelles données sont communiquées à des prestataires tiers et quel usage en font ces derniers. En règle générale, il s'agit de partenaires commerciaux qui ne sont pas des tiers «véritables» au sens de la nLPD. Dans le domaine de l'open banking et l'open finance, la banque peut dès lors leur transmettre des données sans obtenir le consentement préalable du client. La question du consentement ne se pose qu'en cas de transmission de données à des tiers «véritables», et ce en raison du secret professionnel du banquier (voir chapitre 2.3).

https://www.swissbanking.ch/fr/telechargements

2.2 Profilage

Au sens de la nLPD (art. 5, let. f et g), on entend par «profilage» le traitement automatisé de données personnelles en vue d'évaluer certains aspects personnels relatifs à une personne physique comme son rendement au travail, sa situation économique, sa santé, ses préférences, sa localisation ou ses déplacements. Le traitement de données, en particulier l'établissement de corrélations, permet d'analyser puis de prédire avec une certaine vraisemblance des caractéristiques et des modes de comportement propres à des personnes ou à des groupes de personnes.

«S'agissant des prestataires de services financiers, on retiendra que tout profilage à risque élevé doit donner lieu à une analyse d'impact relative à la protection des données personnelles.»

Par exemple, le traitement automatisé de données issues du trafic des paiements permet d'évaluer le comportement de paiement d'un client et ainsi, dans le cadre de la prévention des fraudes, de détecter immédiatement les anomalies dans ses ordres de paiement et de suspendre ces derniers pour protéger à la fois le client et la banque (voir chapitres 3.1 et 3.5). Le profilage peut aussi servir à personnaliser et cibler le marketing (voir chapitre 3.5).

Ces possibilités sont d'autant plus utiles que la nLPD facilite le profilage. Ainsi, sous réserve d'autres prescriptions relatives au secret professionnel du banquier, un profilage peut être effectué à l'échelle d'un groupe sans exigences supplémentaires, car les entreprises appartenant au même groupe ne sont pas considérées comme des tiers au sens de la nLPD (art. 26, al. 3 et art. 31, al. 2, let. b nLPD).

La nLPD introduit par ailleurs une variante du profilage, à savoir le «profilage à risque élevé» défini en ces termes: «tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique» (art. 5, let. g nLPD). Cette formulation reprend de nombreux aspects qui, en fin de compte, valent pour n'importe quel profilage, de sorte qu'elle n'établit pas de distinction claire par rapport au profilage «normal». Les critères définissant un profilage à risque élevé au sens de l'art. 5, let. g nLPD devront être précisés dans la pratique.

S'agissant des prestataires de services financiers, on retiendra que tout profilage à risque élevé doit donner lieu à une analyse d'impact relative à la protection des données personnelles (art. 22, al. 1 et 2 nLPD). En outre, il convient d'atténuer le risque inhérent à ce traitement de données par des MTO (voir chapitre 2.4).

2.3 Motifs justificatifs

Dans la plupart des cas, la banque n'est pas tenue d'obtenir l'accord du client pour traiter des données. En vertu du droit suisse relatif à la protection des données, le traitement de données personnelles est autorisé en principe sans le consentement de la personne concernée ou un autre motif justificatif, pour autant qu'il n'y ait pas ou qu'il ne risque pas d'y avoir d'atteinte à la personnalité. Un risque d'atteinte à la personnalité est présent en particulier lorsqu'un traitement de données enfreint les principes appli-

cables en matière de protection des données, notamment les principes de limitation des finalités, de transparence, de licéité ou de proportionnalité (p. ex. sous l'angle de la parcimonie). Constituent des motifs justificatifs au sens de la nLPD le consentement de la personne concernée, un intérêt privé ou public prépondérant ou une obligation légale de procéder à un traitement de données.

Deux exemples faisant intervenir le principe de limitation des finalités illustrent ci-après l'importance pratique de la question de la justification. A cet égard, il convient de distinguer entre le consentement au sens du droit des contrats (Code des obligations, CO), le consentement au sens du droit pénal (en relation avec le secret professionnel du banquier) et le consentement au sens du droit relatif à la protection des données.

Si la banque collecte des données de clients aux fins de remplir ses obligations contractuelles, elle n'est autorisée à les utiliser à d'autres fins sans le consentement du client concerné que si cela se justifie par ailleurs. La lutte contre le blanchiment d'argent constitue un tel motif justificatif, puisqu'il s'agit d'une obligation légale de la banque. De même, utiliser des données personnelles aux fins d'inviter des clients à une manifestation qui leur est destinée se justifie en général par un intérêt privé prépondérant de la banque, de sorte que c'est autorisé sans le consentement des clients concernés. Cette approche réglementaire de la protection des données est à l'inverse de celle adoptée par le droit européen. En effet, en vertu du Règlement général de l'Union européenne sur la protection des données (RGPD), tout traitement de données personnelles est en principe interdit, sauf à être justifié par une autorisation légale.

Globalement, plus un traitement de données recèle de risques pour les personnes concernées, plus les exigences quant à la validité du consentement au sens du droit relatif à la protection des données doivent être strictes. Lorsqu'un tel consentement est requis de la part du client, il peut revêtir deux formes:

- **consentement tacite:** en application de principes juridiques établis comme par exemple le principe de la bonne foi (art. 6, al. 2 et 3 nLPD), le consentement peut être donné tacitement, c'est-à-dire par un comportement non équivoque du client, dès lors que ce dernier a été dûment informé et agit de son plein gré. On considère ainsi qu'il y a consentement tacite, par exemple, lorsque le client a été informé de nouvelles dispositions contractuelles et ne s'y est pas opposé dans le délai prescrit [8].
- **consentement exprès:** le consentement exprès n'est requis que si la nLPD le prévoit. Il suit lui aussi les règles définies par le CO. En d'autres termes, la manifestation de volonté doit résulter directement des mots employés ou des signaux émis par le client (art. 1, al. 2 CO). Toutefois, l'exigence d'un consentement exprès résultant du droit relatif à la protection des données ne correspond pas à l'exigence de la forme écrite résultant du CO. Selon la nLPD, les éléments déterminants sont que le consentement soit donné sur la base d'informations appropriées, qu'il soit libre quant à son objet, qu'il soit sans équivoque et, pour des raisons de preuve, qu'il puisse être documenté. Dès lors, moyennant une infrastructure contractuelle adéquate et une information transparente et pertinente du client, le consentement exprès peut résulter aussi de l'acceptation des Conditions générales (CG) de la banque ou encore, dans un contexte numérique, du simple fait de cliquer sur un bouton prévu à cet effet.

8 Le consentement nécessitant une déclaration de volonté expresse du client, souvent appelé opt-in, joue un rôle considérable dans le contexte du droit relatif à la protection des données.

Quant à savoir s'il y a lieu, dans un cas donné, d'obtenir un consentement exprès ou tacite, cela ressort des dispositions du code des obligations (art. 1, al. 2 CO).

Les banques doivent vérifier par ailleurs si, au-delà du droit relatif à la protection des données, d'autres exigences sont à respecter en matière de consentement. Les données personnelles de clients étant couvertes par le secret professionnel du banquier, certaines formes de traitement nécessitent que le client consente à la levée du secret avant que la banque soit autorisée à transférer des données à des tiers qui ne sont pas ses mandataires. Les conventions existantes entre les banques et leurs clients peuvent prévoir d'autres exigences en matière de consentement.

Quoiqu'il en soit de la licéité d'un traitement de données, se pose la question des éventuels risques de réputation. Ceux-ci surviennent lorsqu'il existe un écart entre le traitement de données tel que peut l'attendre la personne concernée en vertu du principe de la bonne foi et celui qu'effectue la banque dans les faits. Afin de prévenir un tel écart, il convient de mettre en place un processus d'analyse du risque dans lequel des parties prenantes issues de différents domaines définissent une stratégie en matière de gestion des traitements de données. Ce processus devra préciser quels sont les traitements de données qui, dans le cadre légal autorisé, sont de nature à préserver la réputation de la banque compte tenu de son positionnement sur le marché et quels sont ceux dont il faut s'abstenir pour des raisons de réputation.

2.4 Mesures techniques et organisationnelles (MTO)

Généralités
Les MTO sont des prescriptions visant à permettre le respect des obligations légales. On commence par identifier les prescriptions légales pertinentes, après quoi des experts les transposent dans des prescriptions à vocation opérationnelle: les MTO. Lorsque des mesures techniques produisent des effets nuls ou insuffisants, il convient de prévoir des mesures organisationnelles compensatoires sous forme de MTO [9].

Les MTO tiennent donc dûment compte de l'organisation de la banque concernée en termes de structure et de processus. Elles se fondent sur les règles de la profession, sur l'état de la technique ainsi que sur les normes ou les usages de la branche, de sorte qu'elles évoluent avec leur époque de manière dynamique. Pour ces raisons, elles doivent faire l'objet de contrôles réguliers quant à leur adéquation et à leur efficacité. Cette approche correspond aux principes de protection des données dès la conception (privacy by design) et par défaut (privacy by default) (art. 7 nLPD et art. 25 RGPD). Elle consiste à mettre en place des MTO telles que les traitements de données respectent en particulier les principes de protection des données comme la limitation des finalités, la transparence, la licéité et la proportionnalité (p. ex. sous l'angle de la parcimonie). Elle doit être appliquée dès la planification, c'est-à-dire dès la phase de conception.

9 La présente publication se borne à présenter certaines MTO. On trouvera un aperçu complet de ces mesures dans le Guide relatif aux mesures techniques et organisationnelles de la protection des données publié par le Préposé fédéral à la protection des données et à la transparence (PFPDT).

Exemples généraux de MTO [10]:

- En matière de **confidentialité**, d'**intégrité** et de **disponibilité**, on peut se référer aux prescriptions de la FINMA sur les risques opérationnels et les CID (Circ.-FINMA 2008/21 «Risques opérationnels – banques», en particulier l'annexe 3) ainsi qu'aux normes ISO générales.
- Sur des aspects comme l'**exactitude**, la **limitation des finalités**, la **parcimonie** ou le niveau de **transparence**, il est judicieux d'élaborer des plans opérationnels prévoyant à la fois des prescriptions spécifiques aux applications concernées et des **contrôles** de la gestion des données.
- Peuvent aussi constituer des MTO les prescriptions applicables aux interfaces graphiques (Graphical User Interfaces, GUI), pour régler par exemple les **traitements de données** (limitation des finalités, parcimonie) dans le cadre de zones de texte libre.
- Autre exemple: les prescriptions concernant l'**infrastructure informatique** en général (p. ex. sa **disponibilité**, sa **robustesse**, sa **capacité** et les **preuves de son efficacité**) et plus spécifiquement les interfaces techniques, qui définissent un échange de données au sein de la banque ou avec des prestataires externes en termes de catégories de données, de limitation des finalités, d'exactitude, de parcimonie, etc.
- Parmi les mesures organisationnelles typiques susceptibles d'être prises pour atténuer les risques, en particulier faute de mesures techniques appropriées, figurent par exemple **l'attribution stricte des droits d'accès aux données selon la fonction**, le principe du **double regard**, l'**accès limité à ertaines données** ou l'**obligation d'obtenir une autorisation préalable** pour traiter certaines données.

Exemples concrets de MTO

La protection des données personnelles est assurée par des MTO appropriées en matière de sécurité (informatique), qui visent à préserver la confidentialité, l'intégrité et la disponibilité des données. D'autres MTO potentiellement similaires émanant d'autres domaines spécialisés de l'entreprise (1st line of defense) visent à assurer le respect des dispositions du droit relatif à la protection des données et de celles régissant le secret professionnel du banquier. Par exemple, les MTO d'anonymisation ou de pseudonymisation permettent de supprimer (partiellement) le lien de rattachement à des personnes précises, de sorte que les dispositions du droit relatif à la protection des données et celles régissant le secret professionnel du banquier ne s'appliquent plus.

A l'heure actuelle, les principaux procédés techniques sont les suivants:

- **anonymisation:** l'anonymisation de données consiste à modifier de manière irréversible des attributs personnels (p. ex. le nom et d'autres éléments d'identification d'une personne) de telle sorte qu'ils ne puissent plus être rattachés à cette personne. Dans le cadre du droit relatif à la protection des données, l'anonymisation se traduit par le fait que les personnes concernées ne sont ni identifiées, ni identifiables. Dès lors que les données sont correctement et intégralement anonymisées (c'est-à-

10 On trouvera d'autres exemples de MTO dans les lignes directrices publiées par divers prestataires de services informatiques ou par des autorités de surveillance. Ces modèles sont toutefois à manier avec prudence. En effet, ils se réfèrent souvent exclusivement au RGPD et/ou au droit européen, en omettant des différences significatives quant au cadre juridique général et aux prescriptions sectorielles propres au droit suisse. Sous cette réserve, ces lignes directrices peuvent constituer une source d'inspiration utile, en particulier (en allemand) la «Datenschutz Sachsen-Anhalt Checkliste TOMs nach DSGVO» et le document intitulé «Das Standard-Datenschutzmodell (SDM) - ULD».

dire que les personnes concernées ne sont ni identifiées, ni identifiables), il est incontestable que l'on n'est pas en présence de données personnelles (voir chapitre 2.1).

- **pseudonymisation:** la pseudonymisation consiste non pas à supprimer certains attributs dans un bloc de données, mais à les masquer ou à les remplacer par un nom d'emprunt, appelé pseudonyme, par des caractères ou par un code. L'objectif est d'exclure toute identification de la personne concernée. Les données pseudonymisées ne peuvent donc pas être rattachées directement à une personne, le rattachement s'effectue via une règle de rattachement et/ou une clé. Dès lors que le destinataire des données traite ces données sans disposer de la clé, ce ne sont pas des données personnelles qu'il traite. En conséquence, les données pseudonymisées ne sont anonymisées que du point de vue de leur destinataire. Le responsable des données, quant à lui, peut les rattacher aux personnes concernées à l'aide de la clé en sa possession.
- **cryptage ou chiffrement:** le cryptage consiste à transformer des données personnelles en un «texte codé» à l'aide d'une clé de cryptage. Dès lors, les informations initiales ne sont lisibles que si l'on dispose de la clé de cryptage. L'accès à cette dernière doit être placé sous le contrôle de la banque et protégé des personnes non autorisées. Le processus de cryptage ainsi que la puissance de la clé de cryptage doivent être conformes aux normes de sécurité en vigueur, de sorte que le cryptage puisse être considéré comme cryptographiquement sûr. Toute transmission de CID devrait donc faire l'objet d'une protection spécifique à l'aide de MTO appropriées comme par exemple le cryptage. Au vu de ce qui précède, le cryptage n'est pas un procédé autonome, mais une application technique de la pseudonymisation.

2.5 Gouvernance de l'IA

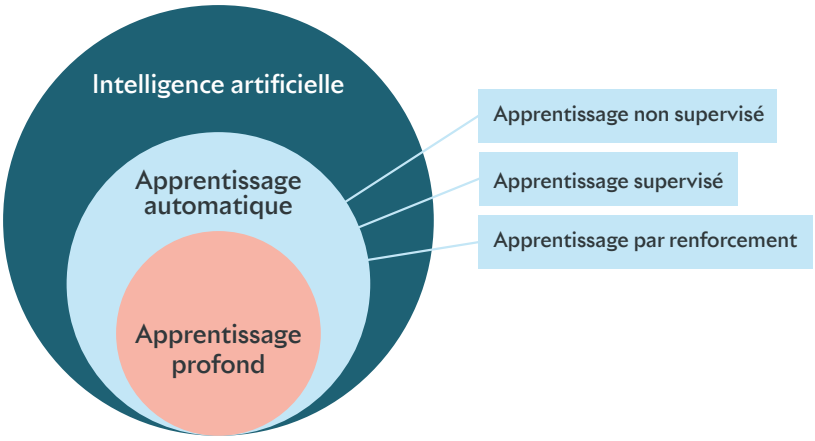
- L'IA compte parmi les sujets qui, ces prochaines années et pour un nombre croissant de banques, seront au cœur de la réflexion sur la gestion des données. La notion d'IA est apparue pour la première fois en 1956, lors d'une conférence au Dartmouth College [11]. Le développement fulgurant que connaît l'IA actuellement s'explique en particulier par l'augmentation de la puissance de traitement informatique au cours des quinze dernières années, ainsi que par la facilité d'accès à des volumes considérables de données d'apprentissage pour les algorithmes autoapprenants. L'IA, qui comprend diverses méthodes, se subdivise en sous-domaines [12]:
- **intelligence artificielle:** domaine de recherche interdisciplinaire visant à faire acquérir des comportements intelligents à des machines (ordinateurs).
- **apprentissage automatique (machine learning):** sous-domaine de l'IA qui consiste à utiliser des algorithmes pour déterminer un modèle à partir de données. Parmi les méthodes d'apprentissage automatique figurent l'apprentissage supervisé (supervised learning), l'apprentissage non supervisé (unsupervised learning) et l'apprentissage par renforcement (reinforcement learning).
- **apprentissage profond ou en profondeur (deep learning):** sous-domaine de l'apprentissage automatique qui permet aux ordinateurs de reconnaître des modèles encore plus complexes (p. ex. à partir de données non structurées comme les signaux audio et vidéo, l'image ou le texte). Cet apprentissage est dit «profond» en raison du fait que ces réseaux neuronaux artificiels comprennent plusieurs couches.

11 Voir P. McCorduck (1979), «Machines Who Think».

12 Voir T. Appenzeller (2017), «The AI revolution in science».

Graphique 3

L'intelligence artificielle et ses sous-domaines



Source: ASB, d'après les travaux du Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle (High Level Expert Group on AI, HLEG) de l'UE

En matière d'IA, les aspects suivants sont particulièrement importants:

- les **blocs de données** utilisés doivent être **de qualité et différenciés**, car des données erronées ou indifférenciées risquent de générer des résultats faux ou discriminants;
- les **processus** basés sur l'IA doivent être **explicables, c'est-à-dire transparents et traçables**;
- le **personnel** bancaire concerné doit être **dûment formé**, afin de pouvoir contrôler si les résultats obtenus automatiquement se situent dans la fourchette prédéfinie et d'être en mesure d'intervenir dans les processus pour remédier à d'éventuels dysfonctionnements.

En ce qui concerne la nature du traitement de données (traitement au moyen d'applications d'IA), il convient de vérifier si, outre le devoir général d'informer résultant du droit relatif à la protection des données (art. 19 et 20 nLPD), le respect de la confiance des clients et le principe de transparence imposent des exigences supplémentaires en matière d'information. Des mesures d'information adéquates peuvent également être utiles pour prévenir un éventuel risque de réputation.

Pour des raisons de contrôle, les décisions concernant les résultats obtenus grâce à l'IA sont le plus souvent réservées aux collaborateurs de la banque. S'il devait arriver que les décisions soient prises exclusivement par des systèmes d'IA, sans intervention d'un collaborateur de la banque, il y aura lieu d'examiner leurs éventuelles conséquences juridiques au regard des dispositions sur les décisions individuelles automatisées (art. 21 nLPD) et, le cas échéant, d'en tenir compte. Si des sous-traitants de la banque ont accès à des données personnelles dans le cadre de l'utilisation de systèmes d'IA et/ou traitent de telles données par ailleurs, il convient de s'assurer du respect du droit relatif à la protection des données en matière de sous-traitance (p. ex. art. 9 nLPD) et, le cas échéant,

«Pour des raisons de contrôle, les décisions concernant les résultats obtenus grâce à l'IA sont le plus souvent réservées aux collaborateurs de la banque.»

en matière de communication de données personnelles à l'étranger (art. 16 ss nLPD). On notera à cet égard qu'un sous-traitant n'est pas un tiers «véritable» au sens de l'art. 31, al. 2, let. c nLPD et que dès lors, le consentement du client au sens du droit relatif à la protection des données n'est pas requis même si ce sous-traitant a accès à des données personnelles sensibles. De plus, le devoir d'informer les personnes concernées est restreint (art. 20, al. 3, let. c, ch. 2 nLPD).

l'IA responsable (responsible AI)

Les nouvelles technologies de l'IA peuvent exposer l'utilisateur à de nouveaux risques, comme les biais (bias), les enjeux éthiques, les résultats non contrôlables et/ou non explicables (black box), le manque de robustesse face à de nouvelles données ou le piratage. Recourir aux technologies de l'IA suppose donc de trouver un équilibre entre innovation et propension au risque. Afin d'identifier, d'évaluer, de prévenir et de contrôler ces risques, il est recommandé d'adopter une approche fondée sur les risques. Les dispositifs d'analyse des risques inhérents à l'IA portent en général sur les quatre domaines suivants:

1. **Gouvernance** (p. ex. gouvernance informatique, gouvernance des modèles, évaluation juridique et compliance, rôles et responsabilités, ethik boards)
2. **Gestion des données** (p. ex. protection des données, droits d'accès, qualité des données, contrôle des données)
3. **Principes, lignes directrices et code de conduite en matière d'IA** (p. ex. explicabilité, équité et égalité de traitement, transparence, éthique, sécurité, contrôle, robustesse et obligation de rendre compte)
4. **Communication, formation et sensibilisation** (p. ex. examens par les pairs, formations pour le personnel, observation du regard extérieur grâce à des radars de tendance en matière d'éthique)

L'IA responsable est un domaine de recherche interdisciplinaire intégrant notamment des questions techniques, économiques, juridiques, sociologiques et philosophiques. Ces dernières années, d'importants progrès ont été réalisés dans tous ces domaines (p. ex. en matière d'explicabilité des algorithmes, d'équité de l'IA, de chiffrement et de cryptographie). D'autres avancées majeures sont attendues dans les années à venir. En parallèle, nombreux ont été les Etats, les organisations internationales de normalisation, les entreprises et les associations sectorielles à développer leurs propres lignes directrices pour le recours à l'IA. Plusieurs initiatives visant à concrétiser ces lignes directrices et à les rendre opérationnelles sont en cours. L'IA connaissant des évolutions fulgurantes, l'ASB recommande aux collaborateurs des banques en charge de ce domaine de se tenir régulièrement au courant et de suivre les travaux de recherche.

Dès lors que des prestataires externes sont amenés à traiter des données de clients, il convient de respecter les conditions légales applicables au recours à des mandataires en vertu du secret professionnel du banquier (art. 47 LB). Il convient également de vérifier si la Circ.-FINMA 2018/3, «Outsourcing», est applicable [13]. Le guide «Cloud» de l'ASB peut être utile pour préciser les prescriptions susmentionnées, dans la mesure où il examine en détail les aspects juridiques pertinents en matière de communication de données à des tiers (p. ex. à des prestataires de cloud computing).

3 Cas concrets

3.1 Recours à l'intelligence artificielle à des fins de compliance

Contexte

Dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme, les banques analysent en permanence un grand nombre de données de clients. En vertu des obligations de diligence que leur impose la loi, elles collectent, documentent et traitent des données personnelles telles que le nom, la date de naissance, les coordonnées, la copie d'une pièce d'identité, le cas échéant des informations sur la situation patrimoniale du client concerné, ainsi que des données de transaction. La source principale de ces données demeure le client lui-même. Toute-fois, à titre complémentaire, les banques recourent aussi à diverses autres sources, comme les bases de données de prestataires spécialisés ou encore Internet.

«Lutter efficacement contre le blanchiment d'argent et le financement du terrorisme est essentiel pour l'intégrité de la place financière suisse.»

Pour les traitements de données liés à la lutte contre le blanchiment d'argent et le financement du terrorisme, les banques peuvent faire appel à des solutions basées sur l'IA et, en particulier, sur l'apprentissage automatique (voir chapitre 2.5). L'avantage de ce dernier réside dans la capacité d'apprentissage des systèmes, qui leur permet d'identifier de nouveaux domaines de risque ainsi que de nouveaux modèles de blanchiment d'argent et de financement du terrorisme. En outre, grâce à l'apprentissage automatique, les analyses sont plus rapides et, au besoin, elles intègrent plusieurs sources de données dont elles assurent un traitement complet et homogène. En règle générale, le recours à cette technologie vise non pas à substituer la machine à l'homme, mais à organiser les processus exigés par la loi de manière plus durable et plus performante. Les décisions continuent d'incomber au collaborateur de la banque qui en a la charge.

Lutter efficacement contre le blanchiment d'argent et le financement du terrorisme est essentiel pour l'intégrité de la place financière suisse. Cela contribue à sa bonne réputation, qui joue un rôle important dans le positionnement international de la Suisse – par exemple au sein du Groupe d'action financière (GAFI). Ce dernier, en fixant des principes internationaux, sert avant tout à protéger les clients des

13 Cas où, dans le cadre des systèmes d'apprentissage automatique, un prestataire a accès à des volumes de données de clients constituant des «grandes quantités de CID» au sens de la Circ.-FINMA 2008/21 «Risques opérationnels – banques» (annexe 3, Cm 53*) et où la banque considère en outre la prestation fournie comme essentielle.

banques, car seul le respect de ces principes communs permet d'assurer la parfaite exécution des transactions internationales.

Applications possibles

Les applications basées sur l'apprentissage automatique peuvent être utilisées à différents stades du cycle de vie des clients:

- **KYC et onboarding:** dans ce cadre, l'IA facilite l'identification automatique des données pertinentes ainsi que l'élaboration des rapports relatifs aux risques. Les systèmes basés sur l'IA reconnaissent les personnes, les lieux, les faits, les événements et les compilent selon des modèles dynamiques créés par auto-apprentissage. Par ailleurs, ils filtrent et recoupent les informations identiques ou similaires et signalent les risques potentiels. Cette préparation efficace des informations nécessaires aux prises de décision permet aux spécialistes internes à la banque de se focaliser sur les sources pertinentes et ainsi de trancher sur des bases solides.
- **surveillance des transactions: l**es systèmes traditionnels de surveillance des transactions identifient les cas suspects uniquement en fonction de règles appliquées par exemple au montant ou à la fréquence des transactions. Si le seuil de divergence retenu est trop élevé, le taux de faux positifs risque d'augmenter, multipliant ainsi inutilement les cas douteux que les collaborateurs de la banque devront vérifier. En revanche, si ce seuil est trop bas, certains risques peuvent ne pas être identifiés. Les systèmes basés sur l'apprentissage automatique, quant à eux, identifient de manière autonome les variations inhabituelles des volumes de transactions et les analysent en corrélation avec d'autres critères de surveillance, comme par exemple la provenance (Etats présentant des risques accrus), la vitesse des transferts d'actifs, l'existence de sanctions, l'implication de PPE[14], le terrorisme. Cette méthode dynamique présente deux avantages principaux par rapport aux systèmes statiques traditionnels: d'une part, l'analyse est plus différenciée et plus flexible, d'autre part, la réduction des faux positifs génère des gains de temps qui sont cruciaux dans ce domaine.

Problématiques éventuelles

Les considérations générales du chapitre 2.5 concernant le recours à l'IA sont à valider au cas par cas. La banque doit évaluer le risque inhérent à l'utilisation de l'apprentissage automatique puis, idéalement, élaborer un plan opérationnel. Il lui appartient en particulier de documenter les MTO adaptées à sa situation (voir chapitre 2.4), qui seront choisies en veillant notamment au respect des principes du droit relatif à la protection des données comme la limitation des finalités, la transparence, la licéité et la proportionnalité (p. ex. sous l'angle de la parcimonie). Il convient par ailleurs de tenir compte du risque lié au type de données et/ou au type de traitement, par exemple en présence de données personnelles sensibles (en particulier, données relatives à des poursuites administratives ou pénales ou à des sanctions) ainsi qu'en cas de profilage et, plus encore, de profilage à risque élevé (voir chapitres 2.1 et 2.2).

Il est bon également que la banque mette en place des processus permettant de s'assurer que les collaborateurs impliqués surveillent le bon fonctionnement des systèmes et sont en mesure de plausibiliser les résultats obtenus (voir chapitre 2.5).

14 PPE est l'abréviation de «personne.s politiquement exposée.s».

On notera enfin que les décisions prises exclusivement sur la base d'un traitement de données personnelles automatisé (décisions individuelles automatisées) sont soumises aux dispositions de l'article 21 nLPD. Il est donc d'autant plus judicieux de mettre en place des processus où les collaborateurs ne soient pas seulement tenus de surveiller les systèmes, mais disposent aussi de compétences décisionnelles (voir chapitres 2.5 et 3.2).

3.2 Examen de crédit

Contexte

Les banques peuvent se procurer, sous forme de données vérifiées, des informations utiles pour évaluer correctement la demande de crédit d'un client. Ces informations supplémentaires leur permettent d'identifier les risques potentiels en amont et de les intégrer dans la contribution au risque[15]. Dès lors, les banques sont en mesure non seulement de proposer des offres personnalisées aux clients, mais aussi de mieux gérer les risques et de planifier la constitution et la dissolution de provisions de manière ciblée. Compte tenu des dispositions de l'article 21 nLPD, applicables aux décisions individuelles automatisées, les développements ci-après reposent sur l'hypothèse que la décision d'octroyer le crédit appartient à une personne – en d'autres termes, le processus d'examen de crédit n'est pas entièrement automatisé (voir chapitres 2.5 et 3.1). En pratique, il s'agit là d'un choix stratégique de l'établissement financier concerné.

Applications possibles

Que l'emprunteur soit une entreprise[16] ou un particulier (crédit hypothécaire, crédit à la consommation), l'examen de crédit donne lieu à des collectes de données. Les modalités de ces collectes de données diffèrent toutefois selon le cas. S'agissant d'entreprises, de nombreuses informations sont accessibles au public, qui peut les consulter ou se les procurer. S'agissant en revanche de particuliers, il peut être nécessaire d'obtenir au préalable le consentement du client concerné à la collecte étendue de données auprès de tiers, non pas en vertu de la nLPD (art. 31, al. 2, let. c) mais en raison du secret professionnel du banquier. Grâce à l'évolution technologique fulgurante, il est aujourd'hui possible de mettre en place des processus d'examen de crédit très efficaces et largement numérisés, basés sur l'apprentissage automatique ou le traitement automatique des langues (TAL)[17].

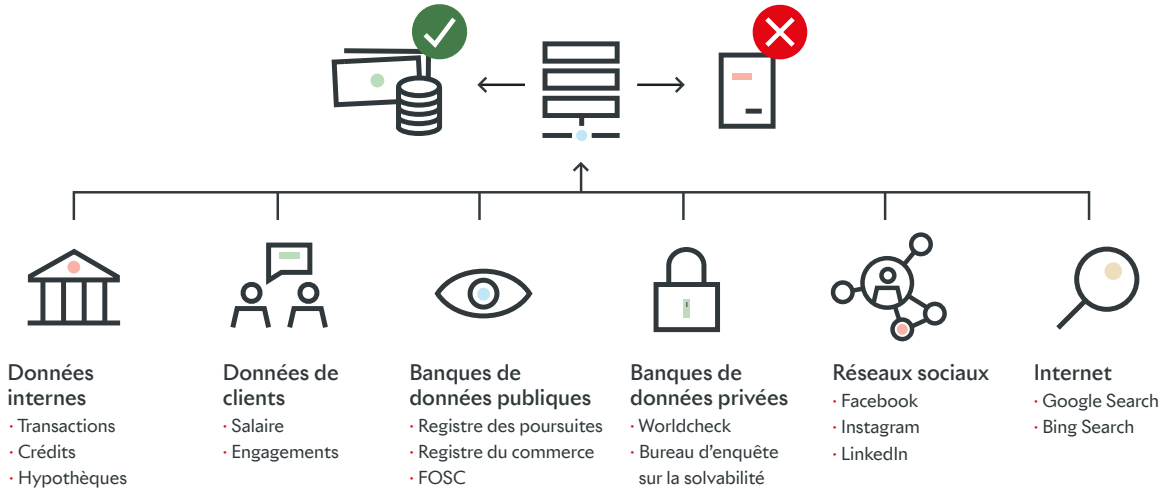
15 Y compris en tenant compte de données comportementales historiques des clients.

16 Hors champ d'application de la nLPD.

17 Le traitement automatique des langues (Natural Language Processing, NLP) est un sous-domaine de l'intelligence artificielle qui vise à rendre le langage naturel intelligible pour une machine, afin que cette dernière puisse traiter et analyser de grandes quantités de données textuelles. Parmi les applications les plus courantes figurent la traduction automatique et la reconnaissance vocale.

Graphique 4

Sources de données possibles (liste non exhaustive)



Source: ASB

Problématiques éventuelles

S'agissant des données utilisées à des fins d'examen de crédit, divers aspects sont à prendre en compte. Tout d'abord, ces données devraient être d'une qualité irréprochable à tout moment. Elles devraient aussi être à jour, refléter correctement la réalité et permettre d'identifier clairement leur source[18]. Au regard du droit relatif à la protection des données et afin d'assurer une qualité parfaite de toutes les données utilisées dans le cadre du processus d'examen de crédit (y compris les données non personnelles), il convient de ne pas traiter les données dont la provenance est douteuse ou qui sont difficiles, voire impossibles à vérifier. Ces problématiques sont prégnantes en particulier lorsque les données sont issues des réseaux sociaux ou d'Internet. Globalement, il est recommandé de communiquer de manière transparente, traçable et claire tant sur le niveau de qualité des données que sur leur provenance. Il peut être judicieux en outre de décrire avec précisions les sources de données utilisées. Par ailleurs, les banques se demanderont avec profit comment informer au mieux les clients pour préserver leur confiance dans le processus (partiellement) automatisé d'examen de crédit et pour assurer à tout moment une gestion fiable des données. Il est enfin essentiel de s'assurer, au moyen de MTO, que le recours à des sources de données externes n'entraîne aucune violation du secret professionnel du banquier et que la collecte, l'analyse et l'utilisation de données dans le cadre de la décision de crédit se limitent aux seules données nécessaires (voir chapitre 2.4).

18 Conformément aux principes de licéité, d'exactitude, d'actualité et de transparence prévus par le droit relatif à la protection des données.

Pour que soient respectés à la fois le cadre légal et l'indispensable relation de confiance avec les clients (notamment les particuliers), il peut être nécessaire le cas échéant que les banques demandent spécifiquement aux clients un consentement exprès à la collecte de données issues de sources externes. Il peut être judicieux également de divulguer les données collectées et utilisées, afin que les fondements de la décision de crédit soient transparents et traçables. Dans l'intérêt d'une gestion optimale des divers risques décrits au chapitre 2, la plupart des données devraient être supprimées en cas de décision de crédit négative et stockées seulement en cas de décision positive, pour justifier cette décision [19]. Le client est protégé par le fait que toute nouvelle demande de crédit entraîne nécessairement une nouvelle collecte de données, dans la mesure où le processus d'examen de crédit doit se fonder sur des données à jour et non sur des données historiques et potentiellement dépassées [20]. Si les approches susmentionnées prévalent déjà dans les relations avec la clientèle Entreprises, elles restent souvent basées sur des processus manuels. Dès lors, dans ce segment, le défi réside avant tout dans l'automatisation judicieuse de ces processus et donc dans les échanges de données (entre banques, etc.) et dans le data staging [21].

3.3 Analyses de tendance et benchmarking

Contexte

La mutation technologique accélère les changements de comportement des clients. Les marchés se décloisonnent de plus en plus. Dans ce contexte, identifier et comprendre en amont les besoins des clients ainsi que leurs nouveaux comportements est un facteur clé de succès, y compris pour les banques. A cet égard, les analyses de tendance et le benchmarking peuvent être de précieux outils. Saisir les tendances à un stade précoce et connaître sa position sur le marché est indispensable pour optimiser sa gamme de produits et organiser en conséquence ses stratégies de distribution.

Applications possibles

Les données de marché, de transaction et de trafic des paiements constituent pour les banques un réservoir de données considérable qui peut être mis à profit dans le cadre d'applications internes comme externes.

19 Il convient de noter que la banque, le cas échéant, pourrait avoir un intérêt privé prépondérant au stockage partiel des données, par exemple en ce qui concerne les coordonnées du client et les motifs pour lesquels la demande de crédit n'a pas abouti.

20 Application des principes d'exactitude et d'actualité prévus par le droit relatif à la protection des données.

21 Compilation, apurement et transformation de données.

Graphique 5

Deux exemples issus du quotidien bancaire

EXEMPLE: ANALYSE DE TENDANCE (INTERNE)

Développement de produits et gestion stratégique de la distribution

Les banques peuvent utiliser des analyses de tendance en interne pour anticiper les changements dans le comportement d'achat des clients(p. ex. hausse ou baisse de la demande concernant certains produits, types de prestations ou canaux de distribution, arrivée de produits de substitution sur le marché). Des systèmes d'alerte précoce leur permettent de gérer stratégiquement leurs ressources en matière de distribution et de mieux exploiter leur réservoir de clients. Identifiés en amont, les tendances et les nouveaux besoins des clients sont intégrés dans le développement de produits et favorisent ainsi l'innovation (p. ex. le développement de solutions de placement ESG).

EXEMPLE: BENCHMARKING (EXTERNE)

Outil de connaissance du marché dans l'e-banking

Les banques disposent de précieuses données sur le marché suisse des entreprises. Elles peuvent les analyser de manière anonymisée puis les mettre à la disposition des clients, par exemple sous la forme d'un outil de connaissance du marché.
Cet outil propose des données agrégées ainsi que des résultats de benchmarking (p. ex. un comparatif de la rentabilité des PME) obtenus à partir de données provenant de différentes sources (p. ex. données de transaction, données de marché ou sources officielles). Ces informations de référence et ces valeurs comparatives sont très utiles pour les entreprises et les aident à gagner en efficacité et en efficience.

Source: ASB

Problématiques éventuelles

La question se pose de savoir quelles données personnelles relatives à quels domaines d'activité la banque peut analyser sans contraintes particulières, c'est-à-dire ce que couvre sa déclaration de confidentialité et comment respecter les principes applicables au traitement des données à l'aide de MTO (voir chapitre 2.4).

L'anonymisation et l'agrégation de données personnelles, en particulier, recèlent un risque résiduel, à savoir la réidentification non intentionnelle de données personnelles individuelles. Dès lors, il y a lieu de s'assurer au moyen de MTO appropriées que tout rattachement de ces données à une personne précise est impossible et que les clients ne peuvent en aucun cas être identifiés (p. ex. par des analyses croisées,

des échantillonnages, ou en combinant les données personnelles avec d'autres données comme des données de clients ou des données accessibles au public)[22].

Le niveau d'agrégation et/ou la taille du groupe nécessaires pour que tout lien avec des personnes précises soit exclu sont à déterminer au cas par cas. Les critères déterminants à cet égard sont notamment le nombre des attributs utilisés, des hiérarchies et des drill-downs ainsi que la taille et la composition de la population de base. En outre, il convient de n'appliquer que des méthodes d'anonymisation sûres et efficaces (reposant sur des méthodes scientifiques récentes[23]) et de ne confier les analyses qu'à des experts reconnus.

Les données utilisées comportent parfois des erreurs systématiques (biais). Celles-ci surviennent par exemple lorsque la clientèle d'une banque n'est pas représentative de la population suisse globale ou du tissu économique. De plus, on peut présumer qu'il existe des chaînes causales apparentes: par exemple, il peut y avoir un lien mesuré statistiquement entre deux valeurs (corrélation) sans qu'il y ait pour autant un lien de causalité. Les avancées scientifiques récentes, comme celles concernant l'équité algorithmique, sont à prendre en compte dans la gestion des données (voir l'infobox «L'intelligence artificielle responsable», chapitre 2.5).

Enfin, les analyses de tendance et le benchmarking devraient être conçus d'emblée de telle sorte que des explications claires puissent être fournies au besoin et que les utilisateurs soient en mesure d'évaluer la pertinence des résultats obtenus par rapport à des problématiques et des domaines d'application précis. Il est recommandé à cet égard d'élaborer un document d'information succinct et transparent, dans le contexte de l'application, sur la composition des blocs de données et les méthodes de traitement utilisées.

3.4 Authentification biométrique

Contexte

Les procédés d'authentification biométrique, comme les empreintes digitales ou la reconnaissance faciale sur smartphone, connaissent un succès croissant, surtout auprès des clients des banques familiers du numérique. Leurs trois atouts principaux sont l'inviolabilité, l'unicité et bien sûr la simplicité du point de vue du client. Ils permettent au secteur financier d'accélérer et de simplifier les processus à l'interface client et constituent en outre un préalable important aux nouveaux modèles d'affaires numériques. Grâce aux évolutions techniques, de nouveaux procédés deviennent intéressants pour les banques, en particulier la reconnaissance vocale. Lors des contacts téléphoniques, celle-ci permet de gagner non seulement en efficacité, mais aussi en confort pour le client, puisque les questions visant à son authentification n'ont plus lieu d'être. Pendant qu'il expose sa demande, le système compare sa voix au profil enregistré auprès de la banque. S'il y a concordance, on passe directement au traitement de la demande.

22 Voir par exemple à cet égard l'avis du groupe de travail européen «article 29» sur la protection des données du 10 avril 2014 (anciennement WP29).

23 Exemples de techniques d'anonymisation et de niveaux d'anonymat et de sécurité: k-anonymat, l-diversité, t-proximité, anatomie, confidentialité différentielle ou utilisation de données synthétiques.

En règle générale, les attributs biométriques ne peuvent être modifiés, de sorte que les données biométriques sont liées à une personne précise et peuvent toujours lui être rattachées [24].

Applications possibles

Elles sont multiples dans le quotidien bancaire. Le procédé d'authentification biométrique le plus approprié se détermine en fonction de l'interaction concrète entre le client et la banque.

Graphique 6

Les procédés d'authentification biométrique dans le quotidien bancaires

Source: ASB

Le plus souvent, le client choisit une fois pour toutes la méthode d'authentification qui s'appliquera dès lors qu'il se connecte à la banque mobile ou à l'e-banking ou qu'il contacte sa banque par téléphone. On constate globalement que l'authentification entièrement numérique donne des résultats tout à fait satisfaisants [25].

Problématiques éventuelles

Il convient de distinguer principalement entre trois procédés d'authentification biométrique: les empreintes digitales, la reconnaissance faciale et la reconnaissance vocale. Souvent, les deux premiers ne nécessitent aucun stockage de données auprès de la banque. En l'état actuel de la technique, les données sont stockées sur le téléphone mobile du client, de sorte que la banque n'est pas soumise aux dispositions légales relatives à la protection des données. S'agissant de l'authentification par les empreintes digitales ou par reconnaissance faciale, la nLPD impose de la transparence, par exemple sous la forme d'une déclaration de confidentialité, mais ne requiert pas le consentement du client. S'agissant en revanche de la reconnaissance vocale, comme l'empreinte vocale et donc les données biométriques du client sont stockées au sein de la banque (on-premises) ou sous sa responsabilité (cloud [26]), les dispositions pertinentes de la nLPD s'appliquent.

24 Les développements du présent chapitre se limitent aux procédés suivants: fingerprint (empreintes digitales), géométrie faciale (reconnaissance faciale) et voice/speech recognition (empreinte vocale et reconnaissance vocale).

25 Voir aussi la Circ.-FINMA 2016/7, «Identification par vidéo et en ligne».

26 Voir le guide «Cloud» de l'ASB.

D'une manière générale, il faut savoir que le stockage de données biométriques (technologie / emplacement du serveur) est soumis aux dispositions légales en vigueur en matière de protection des données – par exemple, pour la personne concernée, le droit d'accès et de rectification ainsi que le droit de désactiver l'authentification biométrique et de supprimer les données y relatives.

Au-delà de l'authentification, un profil biométrique peut aussi servir à déterminer divers attributs comme l'âge, le genre et jusqu'à l'état d'esprit de la personne concernée à un moment donné. C'est pourquoi son usage à des fins d'authentification doit faire l'objet d'une définition exhaustive, toute finalité extérieure à cette définition étant en principe exclue sans l'accord spécifique du client (art.6, al. 3 nLPD). Les exceptions à cette règle (en particulier l'usage du profil biométrique à des fins de poursuite pénale) doivent être prévues par la loi (p. ex. art. 31, al. 1 nLPD, voir aussi chapitre 2 ci-dessus).

«Outre les exigences du droit relatif à la protection des données, le respect des prescriptions concernant le secret professionnel du banquier est naturellement essentiel en matière d'authentification des clients.»

Outre les exigences du droit relatif à la protection des données, le respect des prescriptions concernant le secret professionnel du banquier est naturellement essentiel en matière d'authentification des clients. Aussi la FINMA a-t-elle précisé, dans la Circ.-FINMA 2008/21 «Risques opérationnels – banques» et en particulier à l'annexe 3 de cette dernière, les prescriptions applicables au traitement des données d'identification du client (client identifying data, CID). Comme indiqué plus haut, elle concrétise par des exigences relatives aux MTO l'obligation des banques d'assurer la confidentialité des données d'identification des clients dans un monde numérisé.

Une communication transparente et compréhensible quant au recours à des systèmes biométriques de reconnaissance est de nature à abaisser le seuil d'acceptabilité de ces procédés par les clients ainsi qu'à atténuer d'éventuels risques de réputation. Du point de vue des clients, outre la réputation, le confort d'utilisation est indéniablement un facteur déterminant pour que l'authentification biométrique ne soit pas soumise à l'accord du client en vertu de la loi.

3.5 Offres et conseils personnalisés

Contexte

Les banques tiennent à proposer des offres complètes à leurs clients, en fonction des besoins propres à chacun et en s'appuyant sur des données aussi qualitatives que possible. Lorsque les clients le souhaitent, elles leur fournissent aussi des prestations de conseil ciblées. Dès lors et concrètement, il s'agit pour elles d'individualiser leurs offres de produits et services en fonction des intérêts et des valeurs (p. ex. le développement durable) identifiés chez les clients concernés. A priori, la composition de ces offres est commune à tous les canaux. L'enjeu est notamment d'identifier en amont et de manière aussi systématique que possible les changements de situation importants pour les clients tels qu'ils résultent, par exemple, d'un mariage, d'un divorce, de la naissance d'un enfant, d'un héritage, d'une nouvelle activité professionnelle ou d'un départ en retraite. En effet, de tels changements entraînent souvent de nouveaux besoins en termes de prestations bancaires. Mais attention: lorsqu'on analyse ces situations,

il ne faut pas oublier que des tiers, comme par exemple le ou la conjointe du client, peuvent être concernés également. Ces tiers bénéficient de la protection des données. A condition d'être eux aussi clients de la banque, ils sont protégés en outre par le secret professionnel du banquier. Le cas échéant et au besoin, il y a donc lieu de les intégrer dans le processus en toute transparence, par exemple via le client.

La collecte de données peut s'effectuer de manière entièrement automatisée ou – en principe – de manière entièrement manuelle. Toutefois, les solutions numériques permettent à la banque une approche plus complète, plus efficace et plus ciblée face au client. Une fois mises en œuvre, elles assurent en outre un niveau de qualité identique pour tous les clients (indépendamment de la personne). Plus les blocs de données utilisés sont importants, plus la qualité et la précision s'améliorent. Une collecte de données automatisée et une offre individualisée permettent finalement des prestations de conseil vraiment axées sur le client.

Applications possibles

Les traitements de données permettent d'optimiser dans le temps des offres spécifiques. Par exemple, la banque propose une nouvelle hypothèque à un client juste avant l'échéance d'une hypothèque à taux fixe préexistante et non lorsqu'elle décide de lancer une campagne nationale sur les hypothèques à destination de tous les clients, indépendamment de leurs besoins. Grâce à la collecte systématique de données sur les préférences des clients, elle peut personnaliser son marketing et cibler sa prospection pour promouvoir ses nouveaux produits et services, par exemple lorsqu'elle met un produit de placement innovant sur le marché. Les résultats des analyses peuvent aussi être intégrés directement dans des prestations de conseil, en particulier dans un contrat structuré de conseil en placement, sachant par exemple que le client concerné préfère les placements directs aux solutions de fonds de placement ou qu'il souhaite privilégier les investissements durables. Bien connaître le client, ses préférences, son système de valeurs et sa situation personnelle facilite un suivi optimal répondant à ses besoins et génère ainsi des ventes croisées – sans compter que la banque peut s'appuyer sur les résultats des analyses pour protéger le client en détectant d'éventuelles anomalies dans ses paiements (voir chapitres 3.1 et 3.3). A noter qu'il est possible d'utiliser ces résultats sous une forme anonymisée, c'est-à-dire sans identification possible des personnes concernées, à des fins statistiques ou stratégiques (voir chapitre 2.4).

«Plus les blocs de données utilisés sont importants, plus la qualité et la précision s'améliorent.»

Problématiques éventuelles

La question se pose en particulier de savoir quelles données relatives à quels domaines d'activité la banque peut analyser sans obtenir le consentement préalable du client – en d'autres termes, dans quels cas la transparence suffit. Cela dépend de la nature des données concernées et/ou de la situation concrète (voir chapitre 2).

La banque peut avoir accès à des données de clients dans des circonstances extérieures à son activité bancaire de base. Tel est par exemple le cas lorsqu'elle fournit des prestations de conseil fiscal, raison pour laquelle de nombreux clients, par souci de discrétion, font sciemment appel à une autre banque que leur banque principale pour ces prestations.

On peut alors se demander si et à quelles conditions les données de clients peuvent être utilisées pour proposer des offres personnalisées. Ce qui est tout à fait pertinent et dans l'intérêt du client du point de vue de la banque peut être perçu comme un inconvénient par le client lui-même, soit parce que les offres non sollicitées l'importunent, soit parce que le fait même que la banque traite des données suscite sa méfiance.

Si les exigences fondamentales sont remplies (voir chapitre 2.3) et en vertu du principe de la bonne foi [27], l'analyse de données et le marketing personnalisé en résultant sont toujours autorisés sans contrainte particulière dès lors que les conditions cumulatives suivantes sont respectées:

- l'analyse repose sur des données fournies à la banque par le client lui-même ou collectées auprès de tiers après information du client, et
- les données ont été collectées par la banque dans le cadre de son activité bancaire typique. Cette dernière dépend du modèle d'affaires propre à la banque concernée: s'agissant par exemple d'une banque universelle, elle comprend la tenue de comptes, le trafic des paiements, les opérations de financement et les opérations de placement.

En revanche, si la banque collecte des données de clients dans le cadre d'une activité bancaire non typique, comme par exemple le conseil successoral ou fiscal, il lui appartient de vérifier si l'utilisation de ces données à d'autres fins mais dans le cadre de l'activité bancaire typique requiert des mesures de transparence. Cela se détermine non seulement au regard du principe de la bonne foi, mais aussi au regard des obligations de limitation des finalités et de proportionnalité des traitements de données résultant du droit relatif à la protection des données (art. 6, al. 2 et 3 nLPD). Dès lors que le client déclare ne plus vouloir recevoir d'offres personnalisées, que ce soit en général ou dans certains domaines seulement, la banque est tenue de respecter ce souhait. C'est plus simple dans le cadre d'un système numérique que sur une base purement manuelle. Dans ce contexte, une collecte de données entièrement numérique peut éventuellement être qualifiée de profilage – profilage à risque normal ou à risque élevé selon la sensibilité des données (voir chapitre 2.2). La collecte de données auprès de tiers dans le cadre des conditions générales ne nécessite pas de consentement spécifique préalable du client concerné si les données de ce dernier collectées par la banque entrent dans le champ de son expérience et/ou de ses attentes selon le principe de la bonne foi (voir chapitre 2.3).

Un aspect supplémentaire est à prendre en compte lorsque des collaborateurs de la banque sont présents sur les réseaux sociaux: dans ce cas, pour un conseiller à la clientèle par exemple, les règles internes de la banque concernée en matière de réseaux sociaux s'appliquent en sus des dispositions légales. Ces règles internes définissent les modalités d'accès et d'usage concernant tant les réseaux sociaux que les données qui s'y trouvent.

27 L'art. 5, al. 2 nLPD rappelle expressément l'importance du principe de la bonne foi dans le droit relatif à la protection des données.

3.6 Programmes de fidélité

Contexte
Du point de vue des banques, les programmes de fidélité influent positivement sur les préférences et sur le comportement d'achat des clients puisqu'ils les fidélisent. Ils sont aussi des moyens de se différencier.

Dans le présent guide, on entend par «programmes de fidélité» les outils de fidélisation mis en œuvre par les banques et individualisés à l'aide de traitements de données personnelles. Ces traitements de données peuvent consister par exemple en une analyse de données de clients (comme les paiements) visant à identifier des préférences personnelles.

Les «récompenses» indifférenciées accordées à chaque client de manière identique, par exemple un crédit de CHF 20 à chaque ouverture de compte, n'entrent pas dans le cadre des programmes de fidélité examinés ici, car elles n'exigent aucun traitement de données personnelles.

Applications possibles
Les programmes de fidélité se répartissent en trois grandes catégories:

1. **Remises (cash-back):** les clients d'une banque bénéficient de remises sur les produits de certaines marques correspondant à leurs intérêts personnels et identifiés au vu de leurs opérations financières auprès de cette banque (p. ex. leurs paiements par carte de crédit). Une fois l'achat effectué, la banque crédite la remise sur le compte du client. Ce système permet aux banques de collecter des informations sur les préférences personnelles des clients à partir de leur comportement d'achat.
2. **Systèmes de points avec publicité individualisée:** les clients cumulent des points en fonction des opérations financières qu'ils effectuent auprès de leur banque (p. ex. les paiements par carte de crédit). Ces points leur permettent de faire leur choix dans un catalogue des produits qui, le plus souvent, sont sans relation avec la banque. Les offres sont à la disposition de tous, mais la publicité est personnalisée grâce à l'analyse de données personnelles (p. ex. les données de transaction, qui renseignent sur les comportements d'achat des personnes concernées).
3. **Nouvelles affaires:** les programmes de fidélité permettent d'inciter les clients à faire appel à d'autres prestations de la banque. Par exemple, les opérations par carte de crédit ou les activités de négoce donnent droit à des points qui peuvent ensuite être échangés contre un taux d'intérêt minoré en cas de nouvelle hypothèque, ou contre une meilleure rémunération en cas d'ouverture d'un compte d'épargne.

Les deux premiers types de programmes ont en commun que les banques traitent en interne les données de clients dont elles disposent, mais que la communication de données personnelles à des tiers n'est en principe pas exclue.

Problématiques éventuelles
Les programmes standardisés (c'est-à-dire non individualisés) de fidélisation des clients ne posent guère de problèmes au regard de la protection des données.

En revanche, les programmes individualisés présentés ci-dessus peuvent conduire la banque à collecter et utiliser des données statiques de clients (p. ex. nom, prénom, genre, adresse, numéros de téléphone,

âge, composition du ménage, profession, niveau d'études, numéro de carte, types et données de paiement) ainsi que des géodonnées (p. ex. zone de résidence, distance par rapport à la succursale ou à la filiale la plus proche).

Si ces données sont utilisées à des fins de publicité personnalisée pour des produits de tiers, on sort du cadre de la relation bancaire ordinaire et donc de la finalité de traitement pour laquelle les clients ont initialement communiqué leurs données à la banque. Dans ce cas, la banque est tenue en particulier d'un devoir d'informer qui l'oblige à avertir les clients et à leur fournir des renseignements complets avant leur adhésion au programme de fidélité .

«Les programmes de fidélité peuvent générer de la valeur ajoutée tant pour les clients que pour les banques.»

La banque peut être libérée de ce devoir d'informer si, à l'ouverture de la relation d'affaires, elle a déjà fait savoir au client concerné que des données pouvaient être mises à la disposition de tiers à des fins de publicité personnalisée de leurs produits. En outre, le traitement des données doit être licite, conforme au principe de la bonne foi et proportionné (voir chapitre 2.3). Il ne peut être effectué que dans un but déterminé et identifiable – en l'occurrence, la mise en œuvre d'un programme de fidélité [28].

Les programmes de fidélité peuvent générer de la valeur ajoutée tant pour les clients que pour les banques. Les données collectées par les banques contiennent de précieuses informations, y compris pour les tiers. A l'heure où la commercialisation de ces données en dehors du secteur financier n'est de loin pas à exclure, les clients risquent de craindre que leurs données personnelles soient transmises à des tiers et donc de se montrer sceptiques face aux programmes de fidélité.

Communiquer clairement sur la transmission de données de clients à des tiers, y compris et sur-tout lorsque tel n'est pas le cas, peut être utile à cet égard en suscitant la confiance. Il convient également de vérifier si le consentement préalable du client n'est pas requis en vertu du droit relatif à la protection des données ou, au minimum, en raison du secret professionnel du banquier. S'agissant des programmes de fidélité et de manière générale, le droit relatif à la protection des données, le secret professionnel du banquier (art. 47 LB) et l'annexe 3 de la Circ.-FINMA 2008/21 «Risques opérationnels – banques», qui fournit des précisions quant au traitement des données électroniques de clients, doivent être respectés.

28 Par exemple en leur indiquant clairement, à l'ouverture de la relation d'affaires, que le site Internet de la banque fournit des informations aisément consultables sur le programme de fidélité.

Association suisse
des banquiers
Aeschenplatz 7
CH-4002 Basel
office@sba.ch
www.swissbanking.ch