N

Monthly Newsletter Oct 2024

Droit bancaire et financier

Schellenberg Wittmer

Réglementation de l'IA dans le secteur financier

Grégoire Tribolet

Key Take-aways

1.
La Suisse n'a pas encore introduit de cadre juridique spécifique à l'IA. Les établissements financiers utilisant l'IA doivent se conformer au cadre juridique général et aux attentes de la FINMA en matière de surveillance.

2.
La loi sur l'IA de l'Union Européenne introduit de nouvelles réglementations sur les systèmes d'IA, touchant non seulement les entités de l'UE, mais également les entreprises suisses qui fournissent des systèmes d'IA dans l'UE ou exploitent des systèmes dont les sorties sont utilisées au sein de l'UE.

3.
Les établissements financiers et les entreprises d'assurance doivent adopter un cadre de gouvernance de l'IA et se tenir informés des évolutions réglementaires pour garantir le respect des normes applicables.

1 Introduction

L'intelligence artificielle **(IA)** est devenue un **moteur essentiel de l'innovation dans le secteur financier,** où elle est utilisée dans un large éventail de cas, notamment la détection des fraudes, la gestion des risques, les prévisions de trésorerie, l'automatisation des processus, l'analyse du risque de crédit, la gestion de la relation client, les algorithmes de trading, le développement informatique et l'analyse de l'information. Si les récents développements de l'IA générative offrent des opportunités considérables, ils présentent également des risques. Par conséquent, les régulateurs des marchés financiers augmentent leur surveillance sur les applications d'IA utilisées par les établissements financiers.

Cette newsletter donne un aperçu de l'état actuel du cadre réglementaire suisse applicable aux établissements financiers utilisant des applications d'IA, ainsi que de la loi européenne sur l'IA, qui peut affecter les établissements financiers fournissant des systèmes d'IA à des entités basées dans l'UE ou exploitant des systèmes d'IA dont les sorties sont utilisées au sein de l'UE.

2 Cadre législatif suisse

La Suisse n'a pas encore adopté de cadre réglementaire complet spécifique à l'IA. En 2020, le Conseil fédéral a adopté les lignes directrices sur l'intelligence artificielle pour la Confédération, qui ne s'appliquent qu'à l'administration fédérale. En ce qui concerne le secteur privé, un rapport du Secrétariat d'État à la formation, à la recherche et à l'innovation **(SEFRI)** au Conseil fédéral, publié en 2019, a conclu qu'il n'y avait pas de besoin immédiat d'introduire une législation suisse traitant de l'IA.

Les établissements financiers suisses doivent se conformer aux attentes de la FINMA en matière de surveillance.

Cependant, en 2023, reconnaissant la dynamique croissante en faveur d'une réglementation de l'IA, le Conseil fédéral a chargé le Département fédéral de l'environnement, des transports, de l'énergie et de la communication **(DETEC)** de rédiger un rapport sur les approches réglementaires possibles d'ici à la fin 2024. Ce rapport servira de base à **une éventuelle proposition de cadre réglementaire suisse en matière d'IA en 2025.**

Dans l'intervalle, les entreprises suisses doivent se conformer au **cadre juridique général** lorsqu'elles développent ou exploitent des applications d'IA, telles que la loi sur la protection des données **(LPD)** (voir 2.1 ci-dessous) et les droits de la personnalité, les lois pertinentes sur la propriété intellectuelle et notamment la loi sur le droit d'auteur **(LDA),** ainsi que la loi sur la concurrence déloyale **(LCD)**, conformément à l'approche de la Suisse fondée sur des principes et la neutralité technologique.

En outre, les établissements financiers suisses qui utilisent l'IA doivent répondre aux **attentes de la FINMA en matière de surveillance** (voir 2.2 ci-dessous) et se conformer à d'autres réglementations pertinentes, telles que les dispositions de la loi sur les banques relatives au secret bancaire, la circulaire 2018/3 de la FINMA *(Outsourcing)* et la circulaire 2023/1 de la FINMA (*Risques et résilience opérationnels).*

2.1. Loi sur la protection des données

En novembre 2023, le Préposé fédéral à la protection des données et à la transparence **(PFPDT)** a publié un communiqué soulignant que **la législation suisse sur la protection des données est directement applicable au traitement des données effectué au moyen de l'IA.** La déclaration rappelle aux fabricants, fournisseurs et exploitants d'applications d'IA qu'ils doivent garantir la transparence concernant la finalité, le fonctionnement et la source de données des activités de traitement de données effectuées par l'IA et doivent maintenir le plus haut degré possible d'autodétermination numérique pour les personnes concernées.

Les exigences de la législation suisse sur la protection des données s'appliquent à la plupart des applications d'IA utilisées par les établissements financiers. Les établissements financiers doivent notamment évaluer si l'application d'IA génère des **décisions individuelles automatisées** au sens de l'article 21 LPD. Cette évaluation est particulièrement pertinente pour les applications d'IA utilisées dans le *credit scoring,* l'*onboarding* numérique, la segmentation de la clientèle ou le filtrage des candidatures à un emploi.

Le PFPDT a également souligné que certaines applications d'IA nécessitent une **analyse d'impact relative à la protection des données personnelles** en vertu de l'article 22 LPD. Cela s'applique notamment dans les cas où (i) de grandes quantités de données personnelles sensibles sont traitées, (ii) des données personnelles sont systématiquement collectées à des fins de traitement par l'IA (autrement qu'à des fins statistiques ou non personnelles) ou (iii) les résultats générés par les applications d'IA ont des conséquences importantes pour les personnes concernées.

2.2. Attentes de la FINMA en matière de surveillance

La FINMA suit depuis plusieurs années le développement et l'utilisation de l'IA dans le secteur financier. Au cours des années 2021 et 2022, elle a mené des enquêtes sur l'utilisation de l'IA dans les secteurs de l'assurance, de la banque et de la gestion de fortune, établi un inventaire des domaines dans lesquels des applications d'IA étaient utilisées, et mis en place un service spécialisé d'IA. Dans son monitorage des risques 2023, la FINMA a présenté ses **attentes en matière de surveillance à l'égard des établissements financiers utilisant l'IA,** en se concentrant **sur quatre domaines critiques :**

- **Gouvernance et responsabilité :** Les établissements financiers doivent définir clairement les rôles et les responsabilités pour les décisions liées à l'IA, en veillant à ce que la responsabilité incombe aux humains et non aux systèmes d'IA eux-mêmes. Cela est particulièrement important lorsque les erreurs de l'IA peuvent passer inaperçues, lorsque les processus deviennent trop

complexes ou lorsqu'il y a un manque d'expertise au sein de l'institution.

- **Robustesse et fiabilité :** La précision et la fiabilité des systèmes d'IA doivent être testées, compte tenu notamment des risques de dérive ("drift") des modèles d'auto-apprentissage. Ces systèmes doivent être soumis à des tests rigoureux, en particulier dans les domaines de la gestion des risques. Les systèmes d'IA présentent également des risques en matière de cybersécurité, qui doivent être pris en compte.
- **Transparence et explicabilité :** Les établissements doivent veiller à ce que les systèmes d'IA, en particulier ceux qui affectent directement les clients, soient transparents et que les décisions prises par ces systèmes puissent être comprises et expliquées par les opérateurs humains.
- **Égalité de traitement :** Les systèmes d'IA utilisés dans les services financiers, tels que le *credit scoring*, doivent éviter les biais ou les pratiques discriminatoires. La FINMA exige des établissements qu'ils contrôlent leurs systèmes d'IA afin de prévenir toute forme d'inégalité de traitement.

En publiant ces attentes, la FINMA se met en position d'avant-garde d'une tendance parmi les régulateurs des marchés financiers, qui émettent de plus en plus de directives concernant l'utilisation de l'IA par le biais de *whitepapers*, de lignes directrices ou de communiqués. L'on peut citer à titre d'exemple le communiqué de l'Autorité européenne des marchés financiers **(AEMF)** offrant des directives aux entreprises utilisant l'IA lorsqu'elles fournissent des services d'investissement à des clients de détail (mai 2024), l'article d'expert de l'Autorité fédérale allemande de surveillance financière **(BaFIN)** sur le risque de discrimination dans l'utilisation de l'IA (août 2024), et la mise à jour sur l'IA de la Financial Conduct Authority au Royaume-Uni (avril 2024).

3 Loi européenne sur l'IA

La loi européenne sur l'IA est entrée en vigueur le 1er août 2024 et constitue la **réglementation spécifique à l'IA la plus complète à ce jour.** La loi adopte une approche fondée sur les risques, classant les systèmes d'IA en fonction de leur impact potentiel sur la sécurité et les droits fondamentaux.

3.1 Calendrier

Les dispositions de la loi européenne sur l'IA sont mises en œuvre progressivement sur plusieurs années. Les principales échéances de mise en application sont les suivantes :

2 février 2025	Interdiction des pratiques d'IA présentant des risques inacceptables et exigences en matière de connaissance de l'IA
2 août 2025	Modèles d'IA à usage général (GPAI) et dispositions relatives aux sanctions imposées par les États membres
2 août 2026	La majorité des dispositions de la loi, y compris celles concernant les systèmes d'IA à haut risque et les dispositions relatives à la transparence, entreront en application.
2 août 2027	Mise en place d'une législation sectorielle spécifique à l'IA à haut risque; modèles GPAI déjà sur le marché

Ces périodes de transition donnent aux entreprises le temps de se conformer aux diverses dispositions de la loi, mais il est essentiel de planifier à l'avance, en particulier pour les entités qui utilisent des systèmes d'IA à haut risque.

3.2 Champ d'application territorial

Le champ d'application territorial de la loi européenne sur l'IA est exceptionnellement large, puisqu'il s'applique notamment aux :

- Fournisseurs de systèmes d'IA qui sont mis en service ou mis sur le marché dans l'UE;
- Déployeurs de systèmes d'IA établis dans l'UE; et
- Fournisseurs ou déployeurs de systèmes d'IA dont les sorties sont utilisées dans l'UE.

La loi européenne sur l'IA a un impact sur les fournisseurs et déployeurs de systèmes d'IA établis dans des pays tiers.

Les établissements financiers suisses qui développent ou exploitent des systèmes d'IA peuvent donc être **soumis à la loi européenne sur l'IA,** même s'ils n'ont pas de présence physique dans l'UE, en particulier s'ils (i) développent des systèmes d'IA et les fournissent à des entités basées dans l'UE ou (ii) exploitent des systèmes d'IA produisant des sorties qui sont utilisées dans l'UE (par exemple, par des clients résidant dans l'UE).

Alors que le RGPD s'applique aux entités situées en dehors de l'UE lorsque leurs biens ou services sont au moins partiellement destinés à l'UE, il n'est **pas clair** si la loi européenne sur l'IA s'applique dans les cas où le fournisseur ou le déployeur établi en dehors de l'UE **n'a pas tenté de cibler le marché de l'UE.** Le considérant 22 indique qu'un fournisseur ou un exploitant établi en dehors de l'UE est soumis à la loi si les sorties du système d'IA sont destinées à être utilisés dans l'UE. Toutefois, l'art. 2 para. 1 let. c de la loi européenne sur l'IA n'inclut pas l'élément intentionnel et indique plutôt qu'un fournisseur ou déployeur est soumis à la loi si les sorties du système d'IA sont simplement utilisés dans l'UE.

On ne sait pas non plus comment le **terme "sortie"** sera interprété, mais la loi donne l'exemple de "prédictions, contenus, recommandations ou décisions". Par exemple, les recommandations d'investissement générées par un système d'IA et adressées par un établissement financier suisse à des clients dans l'UE peuvent déclencher l'application de la loi européenne sur l'IA.

En outre, si le fournisseur d'un système d'IA à haut risque est basé dans un pays tiers, il doit désigner un **représentant légal** dans l'UE.

3.3 Catégorisation des systèmes d'IA en fonction des risques

La loi européenne sur l'IA classe les systèmes d'IA en quatre niveaux de risque :

- **Systèmes d'IA interdits :** Il s'agit des systèmes d'IA qui présentent des risques inacceptables, tels que la manipulation de personnes par des techniques subliminales, l'exploitation de vulnérabilités (par exemple, l'âge ou le handicap), ou la création de systèmes de notation sociale qui établissent une discrimination fondée sur le comportement personnel. Ces systèmes d'IA sont interdits par la loi européenne sur l'IA, sous réserve d'exceptions très limitées.
- **Systèmes d'IA à haut risque :** Ces systèmes d'IA sont soumis à des réglementations strictes. Pour les établissements financiers, les systèmes d'IA à haut risque suivants peuvent être particulièrement pertinents :
  - Les systèmes d'IA utilisés pour évaluer la solvabilité des personnes physiques ou établir leur note de crédit (sauf pour détecter les fraudes financières) ;
  - Systèmes d'IA utilisés pour l'évaluation des risques et la tarification dans le domaine de l'assurance-vie et de l'assurance maladie ;
  - Systèmes d'IA utilisés pour le recrutement ou la sélection de personnes, y compris la diffusion d'offres d'emploi ciblées, l'analyse et le filtrage des candidatures et l'évaluation des candidats.
- **Systèmes d'IA à risque limité :** Ces systèmes sont soumis à des exigences de transparence. À titre d'illustration, les systèmes d'IA qui interagissent directement avec les consommateurs (tels que les *chatbots*) doivent informer les utilisateurs qu'ils interagissent avec l'IA. De même, le contenu généré par l'IA (par exemple, les médias synthétiques ou les *deep fakes*) doit être présenté comme tel afin d'éviter toute tromperie.
- **Systèmes d'IA à risque minimal :** Ces systèmes ne sont soumis à aucune exigence réglementaire obligatoire, mais les entreprises sont encouragées à adopter des codes de conduite pour promouvoir une utilisation éthique de l'IA.

3.4 Exigences spécifiques pour les systèmes d'IA à haut risque

Les fournisseurs et les déployeurs de systèmes d'IA à haut risque doivent se conformer à de nombreuses exigences, notamment :

- **Gestion des risques :** Des systèmes complets de gestion des risques doivent être mis en œuvre pour faire face aux risques potentiels tout au long du cycle de vie du système d'IA. Ces systèmes doivent identifier les risques prévisibles pour la santé, la sécurité et les droits fondamentaux et garantir la mise en place de mesures d'atténuation appropriées.
- **Gouvernance des données :** La loi européenne sur l'IA exige que les ensembles de données de formation, de validation et de test pour les systèmes d'IA à haut risque soient représentatifs, pertinents et exempts d'erreurs. Une attention particulière doit être accordée à la prévention des biais dans les ensembles de données, en particulier dans les systèmes touchant les droits fondamentaux, tels que ceux utilisés pour le recrutement ou les analyses de crédit.
- **Transparence et surveillance humaine :** les systèmes d'IA à haut risque doivent être conçus de manière à permettre une surveillance humaine efficace, avec des mécanismes permettant d'interrompre les opérations si nécessaire. Les opérateurs humains doivent être en mesure d'interpréter les résultats du système, de comprendre ses limites et de passer outre les décisions de l'IA si nécessaire.
- **Évaluations de conformité :** Avant de mettre sur le marché un système d'IA à haut risque, les fournisseurs doivent procéder à une évaluation de conformité pour s'assurer que le système répond aux normes réglementaires. Selon le système, des évaluations par des tiers peuvent être nécessaires.

La loi européenne sur l'IA cherche à éviter les chevauchements potentiels entre certaines de ses exigences et celles imposées aux institutions financières par la législation de l'UE en lien avec les services financiers. Par conséquent, les institutions financières qui fournissent ou exploitent des systèmes d'IA à haut risque bénéficient de dérogations limitées dans des domaines spécifiques.

Les systèmes d'IA à haut risque sont soumis à des exigences strictes en vertu de la loi européenne sur l'IA.

3.5 Mécanismes de conformité et d'application

La loi européenne sur l'IA établit une **structure de supervision et d'application à plusieurs niveaux.** Au niveau de l'UE, le Bureau européen de l'intelligence artificielle supervisera la mise en œuvre de la loi, tandis que chaque État membre devra désigner des autorités nationales chargées de faire appliquer la loi dans sa juridiction. Ces autorités auront le pouvoir de surveiller le marché, d'enquêter sur les cas de non-conformité et d'imposer des sanctions. Pour le secteur financier, les autorités compétentes pour la supervision des établissements financiers en vertu des lois sur les marchés financiers devraient également superviser le respect de la loi européenne sur l'IA.

Le non-respect de la loi européenne sur l'IA peut entraîner des **sanctions importantes.** Les entreprises qui se livrent à des pratiques d'IA interdites s'exposent à des amendes pouvant aller jusqu'à 35 millions d'euros ou 7 % du chiffre d'affaires annuel total, selon le montant qui est le plus élevé. Pour les infractions liées aux systèmes d'IA à haut risque et à certains autres systèmes d'IA, les amendes peuvent atteindre 15 millions d'euros ou 3 % du chiffre d'affaires annuel.

4 Conclusion

Bien que la Suisse n'ait pas encore introduit un cadre réglementaire complet spécifique à l'IA, les établissements financiers sont tenus de naviguer dans le paysage juridique général existant, en particulier dans des domaines tels que les droits de la personnalité et la protection des données, et de se conformer aux attentes de la FINMA en matière de surveillance. Ces obligations sont fondées sur des principes et concernent principalement la transparence et la responsabilité liées à l'utilisation de l'IA. Elles sont également pertinentes pour les entreprises d'assurance.

En revanche, la loi européenne sur l'IA établit un cadre réglementaire plus détaillé, plus granulaire et de plus grande portée, qui s'applique non seulement aux entités basées dans l'UE, mais aussi aux fournisseurs ou déployeurs de systèmes d'IA de pays tiers dont les sorties sont utilisées dans l'UE – ce qui pourrait avoir un impact sur les établissements financiers et les entreprises d'assurance suisses. Pour rester en conformité, les établissements financiers et entreprises d'assurance qui utilisent ou prévoient d'utiliser l'IA devraient commencer à adopter un cadre de gouvernance de l'IA et se tenir informés des évolutions réglementaires à venir.

Grégoire Tribolet
Partner
gregoire.tribolet@swlegal.ch

Stéphanie Chuffart-Finsterwald
Partner
stephanie.chuffart@swlegal.ch

Roland Mathys
Partner
roland.mathys@swlegal.ch

Olivier Favre
Partner
olivier.favre@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P.O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.com

Geneva
15bis, rue des Alpes
P.O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.com

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg