



Aspects juridiques de l'intelligence artificielle

Samuel Klaus et Claudia Jung

Résumé des points principaux

- 1.** L'intelligence artificielle (IA) fonctionne en identifiant des schémas types à partir de données non structurées. Elle applique ensuite un algorithme spécifique qui permet de tirer une conclusion.
- 2.** Quels que soient le domaine et le but d'une application utilisant l'IA, des questions juridiques se posent lors de la création, du paramétrage et de l'utilisation de ces applications.
- 3.** La législation actuelle ne tient pas (encore) compte de la complexité induite par l'IA. Les risques juridiques doivent dès lors être anticipés et résolus par des mesures organisationnelles et des dispositions contractuelles ad hoc.

1 Qu'est-ce que "l'intelligence artificielle"?

1.1 Terme

Le terme "**Intelligence Artificielle**" (IA) ne fait pas référence à une technologie spécifique. L'IA est un terme générique qui désigne une multitude de méthodes employant des capacités cognitives simulées à l'aide de modèles mathématiques-statistiques.

1.2 Mode de fonctionnement

Le fonctionnement de l'IA repose sur l'identification de données non structurées (**Big Data**) à l'aide d'un algorithme adapté à une utilisation spécifique et permettant de tirer une conclusion. Pour ce faire, des **réseaux dits neuronaux** (*Neural Networks*) sont mis en place, dont les algorithmes et la structure sont basés sur le fonctionnement du cerveau humain. De nombreux algorithmes individuels fonctionnent ensemble en réseau, sur le modèle de la mise en réseau des synapses dans le cerveau. Les réseaux de neurones complexes avec plusieurs couches de traitement (c'est-à-dire avec de nombreux algorithmes connectés en série et s'influençant mutuellement) sont appelés **Deep Neural Networks**.

Dans les réseaux neuronaux complexes ("profonds"), la façon dont les algorithmes interagissent entre eux n'est plus spécifiée par le développeur, car le nombre de paramètres à définir est beaucoup trop grand. Au lieu de cela, des données d'entraînement appropriées (c'est-à-dire des données d'entraînement adaptées à l'application spécifique, par exemple, des images radiographiques contenant des affections tumorales diagnostiquées) sont soumises au réseau neuronal et traitées au cours d'un grand nombre de cycles d'entraînement automatisés. En même temps, le réseau neuronal utilise des **processus d'optimisation statistique** pour trouver le meilleur "réglage" possible (paramétrage), par exemple pour détecter de manière autonome des affections tumorales sur de nouvelles images radiographiques. Ce processus d'ajustement automatisé du réseau neuronal est connu sous le nom de **Deep Learning**.

La qualité d'une application d'IA dépend de son architecture, de son entraînement et de la qualité des données d'entraînement.

La structure du réseau neuronal et ses paramètres doivent être adaptés **au but de l'application** utilisant l'IA (par exemple, la reconnaissance vocale ou la reconnaissance d'images, la génération de texte, etc.). Idéalement, l'application d'IA sera alors en mesure de reconnaître très rapide-

ment à partir d'une grande quantité de données (p. ex. le flux de données d'une caméra de surveillance) le type de schéma pour lequel elle a été entraînée (p. ex. visages, plaques d'immatriculation, etc.). Son succès dépend de l'architecture du réseau neuronal, de la manière dont il a été entraîné et de la qualité des données d'entraînement.

1.3 Domaines d'application

Les applications utilisant l'IA permettent d'analyser rapidement une grande quantité de données très complexes ou dynamiques (par exemple, les données de cartes de crédit pour la prévention de la fraude, la reconnaissance vocale et d'images en temps réel, l'orientation d'un véhicule autonome en fonction de son environnement).

2 Aspects juridiques

Quels que soient le domaine et le but d'une application utilisant l'IA, des questions juridiques se posent concernant sa **création** (chapitre 2.1), son **paramétrage** (chapitre 2.2) et son **utilisation** (chapitre 2.3).

2.1 Au moment de la création

Lors de la création d'applications utilisant l'IA, les questions relatives à la protection de l'application et à son intégration dans des produits physiques sont particulièrement importantes pour les concepteurs et leurs sous-traitants.

Les logiciels sont protégés par le droit d'auteur, au contraire des algorithmes et des paramétrages. Bien qu'une application utilisant l'IA soit mise en place à l'aide d'un logiciel, elle est largement basée sur des algorithmes et leur paramétrage. Il manque généralement le caractère technique pour pouvoir la protéger. Le cœur d'une application utilisant l'IA ne peut donc être protégé ni par le droit d'auteur ni par un brevet. Le concepteur d'une application utilisant l'IA devrait donc prendre d'autres mesures de protection, par exemple en concluant avec les parties concernées un accord de confidentialité.

Souvent, **les applications utilisant l'IA sont intégrées dans des produits physiques** (p. ex. des appareils, machines, et robots dits intelligents ("smart") qui sont soumis à la législation sur la responsabilité du fait des produits (LRFP) et la sécurité des produits (LSPPro). Il faut alors tenir compte de la complexité supplémentaire résultant de l'utilisation de l'IA (par exemple, dans la surveillance constante de produits basés sur l'IA qui, après leur mises sur le marché, évoluent par interaction avec les utilisateurs).

Les développeurs qui conçoivent des applications utilisant l'IA sont confrontés aux **questions habituelles concernant les contrats dans le domaine des Technologies de l'Information et de la Communication (TIC)**. Un contrat relatif à la conception d'une application utilisant l'IA constitue un contrat d'entreprise pour lequel se posent notamment des questions en lien avec la définition de l'ouvrage et de ses défauts (p.ex. de quelle manière les exigences relatives à l'IA doivent-elles être explicitées, et quand y a-t-il un défaut?) ainsi qu'en matière de responsabilité pour les défauts envers le maître d'ouvrage. Par exemple, le fait de choisir un algorithme pas adapté à l'application souhaitée ou une structure du réseau neuronal pas adaptée à cet usage peuvent-ils constituer un défaut du développeur ? Pour prévenir ces situations, il est conseillé aux parties de préciser dans le contrat les objectifs de l'application à développer, ainsi que les spécificités

telles que définies par le client. Une réglementation précise est également nécessaire dans les cas où le client entraîne lui-même l'application utilisant l'IA ou fournit les données d'entraînement (cf. chapitre 2.2), lorsqu'il souhaite réaliser lui-même des développements futurs de l'application ou encore l'utiliser à des fins autres que celles initialement prévues.

2.2 Pendant l'entraînement (paramétrage)

Le réseau neuronal d'une application d'IA doit être paramétré ("entraîné") sur la base **des données d'entraînement les plus appropriées possibles**. En s'entraînant, il effectue un certain nombre de cycles d'optimisation, jusqu'à ce qu'un réglage optimal ("paramétrage") des différents algorithmes qui composent le réseau neuronal soit atteint. Ce processus soulève des questions relatives à la qualité et à la protection juridique des données d'entraînement, ainsi qu'à la protection des données.

La **sélection et la qualité des données d'entraînement** influencent les résultats de l'application utilisant l'IA en phase de production. Si des données inadéquates sont sélectionnées ou si elles sont de mauvaise qualité (p. ex. si leur structure, leur étendue, et leur contenu ne peuvent être comparés aux données entrées ultérieurement), l'application utilisant l'IA ne produira vraisemblablement pas les résultats escomptés.

En outre, la sélection des données d'entraînement doit répondre à des exigences élevées afin que ne soient pas transférées des tendances préexistantes (et indésirables) dans l'application utilisant l'IA. Comme l'expérience l'a montré, cela est particulièrement important en ce qui concerne les **aspects relatifs à l'égalité et à la non-discrimination**: si les données utilisées pour l'entraînement sont déséquilibrées (par ex. en ce qui concerne le sexe ou la couleur de peau), l'application utilisant l'IA, après avoir été entraînée avec ces données, reproduira ce déséquilibre (appelé "**Machine Bias**" ou "biais automatique"). Si une entreprise utilise une application reproduisant un tel biais, elle court le risque de violer les exigences légales en matière d'égalité et de non-discrimination (voir chapitre 2.3).

Quiconque fait appel à des tiers s'agissant de la phase d'entraînement d'une application utilisant l'IA serait bien avisé d'obtenir des **assurances contractuelles** quant à la composition et à la qualité des données d'entraînement, ainsi qu'à l'adéquation entre l'entraînement et le résultat voulu. Les concepteurs qui effectuent l'entraînement avec des données qu'ils auront eux-mêmes sélectionnées doivent en vérifier la qualité et l'adéquation.

L'entraînement d'une application utilisant l'IA et les données d'entraînement nécessaires sont au moins aussi importantes que le choix de la structure et des algorithmes. Cela pose la question de la possibilité de protéger **les données d'entraînement**. En droit suisse, les collectes de données prises isolément ne peuvent pas être protégées par le droit de la propriété intellectuelle, rendant nécessaires des garanties contractuelles relatives à l'utilisation, la préservation ou encore le droit exclusif d'utiliser des données **d'entraînement**.

Souvent, les données **d'entraînement** contiennent des données personnelles (p.ex. des personnes peuvent être reconnues sur les images). Dans un tel cas, les exigences de la protection des données doivent être respectées, à savoir la loi sur la protection des données (LPD) lorsque seule la Suisse est concernée, et le règlement général sur la **protection des données** (RGPD) si les données s'étendent à l'UE. Si les don-

nées sont fournies par des tiers, des garanties contractuelles doivent être fournies par le tiers s'agissant du respect des lois applicables à leur collecte et à leur traitement. Si le concepteur de l'application utilise des données sous son contrôle, il convient de vérifier si leur utilisation est autorisée: si la personne concernée n'a pas donné son consentement à l'utilisation de données la concernant, elles ne pourront pas être utilisées car l'intention de créer une application d'IA n'est généralement pas suffisante comme justification autorisant l'utilisation de ces données. Dans certains cas, une anonymisation des données d'entraînement peut être une solution.

2.3 Pendant l'utilisation

L'entreprise qui se sert d'une application utilisant l'IA est tout aussi **responsable des conséquences négatives** de celle-ci que si elle utilisait d'autres outils. Même si l'application utilisant l'IA est dans une certaine mesure autonome, et que des dommages sont causés à la suite de l'adoption par l'application d'un comportement autonome, l'entreprise ne peut rien en déduire pour se défendre: une application utilisant l'IA ne dispose pas d'une autonomie juridique, et par conséquent **l'action d'une application utilisant l'IA est toujours attribuée à l'entreprise qui s'en sert**. Cela soulève la question de la responsabilité liée aux décisions fondées sur l'IA et de la possibilité de recours.

Si des dommages sont causés à des tiers par une entreprise suite à l'utilisation d'une application basée sur l'IA, il convient d'en connaître les raisons. Était-ce à cause d'une structure inappropriée du réseau neuronal? D'un entraînement mal exécuté? De données d'entraînement inappropriées? Dans ces cas, la cause du dommage serait dans la sphère de responsabilité du concepteur. Toutefois, s'il s'agit d'une erreur d'usage (p. ex. saisie de données inappropriées) ou si l'application utilisant l'IA a été utilisée à d'autres fins que celles pour lesquelles elle avait été conçue à l'origine, la responsabilité incombe à l'entreprise qui l'utilise sans l'avoir conçue. Dans tous les cas, la condition préalable à l'identification de l'origine de la faute est la **traçabilité** du processus de traitement et de décision de l'application utilisant l'IA (appelée "**Algorithmic Explainability**"). Une entreprise qui utilise des applications se servant de l'IA, qui ont été créées, respectivement entraînées par des tiers, doit donc également obtenir des garanties appropriées et recevoir une documentation adéquate.

Une application utilisant l'IA qui aurait été mal programmée, ou mal entraînée, peut lors de son utilisation aboutir à une violation des principes d'égalité et de non-discrimination. Si, par exemple, des personnes du sexe féminin sont systématiquement désavantagées par des décisions fondées sur l'IA en raison d'un biais de la machine (par exemple en matière d'emploi ou de salaire), il peut également y avoir une violation de la loi sur l'égalité (LEg).

Dans chaque domaine d'application, des **réglementations sectorielles obligatoires** doivent être respectées (par ex. dans le domaine de la circulation routière s'agissant des véhicules automobiles, dans le domaine de la santé pour des produits médicaux à base d'IA, ou encore dans le domaine de la finance s'agissant de la gestion automatisée de portefeuilles). Une application utilisant l'IA doit donc être mise en œuvre de telle sorte qu'elle tienne compte de ces prérequis. Toute personne qui se procure une application utilisant l'IA auprès d'un concepteur tiers doit donc obtenir des garanties appropriées.

Si les applications utilisant l'IA ne sont pas uniquement utilisées comme outil de préparation des décisions, mais aussi afin de prendre des décisions dans le cadre d'un processus automatisé (par exemple pour l'approbation ou le rejet automatisé d'un prêt sur la base d'un contrôle de solvabilité effectué par un outil fondé sur l'IA), les **obligations relatives à la protection des données** doivent également être respectées: dans le champ d'application du RGDP, il est prévu que les personnes concernées ont le droit de ne pas être soumises à une décision fondée exclusivement sur un processus décisionnel automatisé. Ce n'est pas le cas actuellement en application de la LPD, mais l'introduction d'une réglementation similaire est prévue dans le cadre de sa révision.

Si les applications utilisant l'IA sont utilisées pour des **processus créatifs** (par exemple pour la conception de nouveaux produits), il convient d'examiner comment protéger les résultats créés de manière autonome par une application utilisant l'IA. En l'absence d'un créateur humain, de tels résultats **ne peuvent pas être protégés par le droit d'auteur**. Dans le cadre de l'analyse d'une éventuelle protection conférée par la loi sur les

designs (LDes), la question se pose de savoir qui pourrait être considéré comme le "designer": le fabricant de l'application AI? Celui qui procède à l'entraînement? Le fournisseur des données de saisie ou encore la personne qui utilise l'application fondée sur l'AI? Il est donc d'autant plus important de convenir de **dispositions contractuelles appropriées** concernant l'utilisation proprement dite de l'application fondée sur l'IA ainsi que l'exploitation des résultats générés par elle, ou avec l'aide de celle-ci.

3 Conclusion

Les applications fondées sur l'IA peuvent être utilisées de nombreuses façons et présentent un grand potentiel. Elles amènent cependant également leur lot de **risques juridiques**. Dans la mesure où la législation ne tient pas (encore) compte de la complexité induite par les applications utilisant l'IA et des problèmes particuliers qui y sont associés, les risques juridiques devraient être anticipés et résolus par **un processus et un cahier des charges strictes**, ainsi que des **dispositions contractuelles ad hoc** convenues avec les parties concernées.



Louis Burrus
Associé Genève
louis.burrus@swlegal.ch



Olivier Hari
Conseil Genève
olivier.hari@swlegal.ch



Roland Mathys
Associé Zurich
roland.mathys@swlegal.ch



Samuel Klaus
Senior Associate Zurich
samuel.klaus@swlegal.ch

Le contenu de cette Newsletter ne peut pas être assimilé à un avis ou conseil juridique ou fiscal. Si vous souhaitez obtenir un avis sur votre situation particulière, votre personne de contact habituelle auprès de Schellenberg Wittmer SA ou l'une des personnes mentionnées ci-dessus répondra volontiers à vos questions.

Schellenberg Wittmer SA est votre cabinet d'avocats d'affaires de référence en Suisse avec plus de 150 juristes à Zurich et Genève ainsi qu'un bureau à Singapour. Nous répondons à tous vos besoins juridiques – transactions, conseil, contentieux.



Schellenberg Wittmer Ltd
Avocats

Zurich
Löwenstrasse 19
Case postale 2201
8021 Zurich / Suisse
T +41 44 215 5252
www.swlegal.ch

Genève
15bis, rue des Alpes
Case postale 2088
1211 Genève 1 / Suisse
T +41 22 707 8000
www.swlegal.ch

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