Philippe Gilliéron

Réflexions autour de la contractualisation des projets d'intelligence artificielle

Recommandations pratiques

À l'heure où les projets impliquant le recours à des outils d'intelligence artificielle se multiplient, de nombreuses questions se posent quant aux points auxquels le juriste doit faire attention lors de la contractualisation de ces projets. La présente contribution se propose d'en dresser un éventail.

In einer Zeit, in der sich Projekte mit Einsatz von KI-Tools häufen, ergeben sich zahlreiche Fragen in Bezug auf die Punkte, die Juristinnen und Juristen bei der Vertragsgestaltung solcher Projekte beachten müssen. Dieser Beitrag diskutiert eine Auswahl davon.

La présente contribution a pour objectif de proposer au lecteur une grille de lecture des dispositions contractuelles auxquelles il faut s'attacher lors du recours à des outils d'intelligence artificielle («IA»). S'il est exact qu'en bien des hypothèses ces conditions ne seront pas négociables, leur lecture avisée permettra au client de comprendre les risques qu'il encourt en optant pour un fournisseur plutôt qu'un autre, d'apprécier ces risques en connaissance de cause et, le cas échéant, de le guider dans ses choix.

Cette contractualisation doit être pensée à l'aune du cycle de vie des outils IA, lequel commence par la définition d'un besoin susceptible d'être satisfait par l'adoption d'un tel outil. Une fois ce besoin défini, la question se pose de savoir s'il peut être satisfait par un modèle existant ou si le modèle lui-même doit être développé, respectivement «personnalisé», le cas échéant en développant une application greffée sur un outil préexistant.

Nous commencerons par l'hypothèse où le besoin peut être satisfait par un outil existant, avant d'aborder celle où il s'avère nécessaire de développer un nouveau modèle ou, à tout le moins, le «personnaliser» d'une manière ou d'une autre.

Philippe Gilliéron, Prof. Dr. iur., avocat.

I. Outil standard

Lorsqu'un outil standard est disponible, c'est à l'examen des conditions générales proposées par le fournisseur qu'il conviendra de s'attacher.

Sans prétendre à l'exhaustivité, l'examen de ces conditions exige que l'on s'interroge sur les points énumérés ci-dessous. Ces points se veulent généraux. Ne sera en revanche pas examinée ici la question de savoir si de telles conditions générales pourraient ne pas être conformes à des réglementations spécifiques applicables au client suivant l'industrie dans laquelle il exerce son activité. Le client devra donc conserver à l'esprit que, suivant son domaine (par exemple bancaire ou médical), il lui incombe de s'assurer qu'il lui est possible de recourir à un outil déterminé et que son exploitation se fera conformément à la réglementation spécifique qui lui est applicable.

1. Données personnelles

La première question consiste à se demander si des données personnelles, autres que de contacts entre les parties pour la gestion du contrat qui les lie, devront être traitées lors de l'exploitation de l'outil.

En bien des hypothèses, les conditions générales du fournisseur attireront l'attention du client sur le fait qu'il lui incombe de s'assurer qu'aucune donnée personnelle n'est ingérée dans l'outil. Ce faisant, le fournisseur cherchera à ne pas être qualifié de sous-traitant ou, le cas échéant, de responsable conjoint de traitement aux côtés du client.

Lorsque l'exploitation de l'outil se conçoit difficilement au regard de sa finalité sans que des données personnelles ne soient traitées, il conviendra de se demander si leur anonymisation est possible, en particulier au moyen de technologies améliorant la confidentialité, plus connues

sous l'acronyme anglais «PET» *(Privacy-Enhancing Technologies)*. Parmi les technologies existantes régulièrement évoquées à l'heure où j'écris ces lignes, on peut mentionner le recours à des données synthétiques ou la confidentialité différentielle *(differential privacy)*.

Lorsqu'aucune technique d'anonymisation n'est envisageable, ce qui devrait être exceptionnel, il conviendra de veiller au respect des grands principes usuels que sont en particulier celui de la minimisation des données traitées eu égard à la finalité recherchée et le devoir d'information vis-à-vis des individus dont les données sont traitées.

Un accord de traitement en matière de données *(data processing agreement)* devra alors être conclu entre le fournisseur et le client, ce qui exigera que l'on s'attache aux questions usuelles que sont les catégories et types de données personnelles concernées, leur éventuel partage, la finalité de ce partage et l'identité des récipiendaires sans oublier leur localisation et mesures techniques et organisationnelles pour garantir leur confidentialité, intégrité et disponibilité (CIA). Plusieurs autorités nationales en matière de protection des données ont d'ores et déjà émis des recommandations à ce sujet, dont l'ICO au Royaume-Uni[1] et la CNIL en France,[2] cette dernière considérant par ailleurs que la mise sur pied de bases de données aux fins d'entraînement exige l'exécution préalable d'une analyse d'impact au vu des risques qui y sont liés.[3]

Les relations entre ces outils et la protection des données ayant d'ores et déjà fait l'objet de nombreuses contributions,[4] je me permets d'y renvoyer le lecteur sans entrer dans davantage de détails.

2. Licence

Le droit d'accéder et d'utiliser l'outil, dont l'hébergement sera le plus souvent externalisé *(SaaS)*, fera l'objet d'une licence du fournisseur en faveur du client.

Le client devra veiller à ce que l'étendue de la licence lui permette d'atteindre l'objectif visé. Étant donné les risques que peut représenter pour le fournisseur l'utilisation d'un tel système, on peut s'attendre que les clauses définissant les usages autorisés *(AUP, Acceptable Use Policy)* et les restrictions d'utilisation *(Usage Restrictions)* revêtent une importance particulière, et qu'elles s'étoffent au gré de l'imagination des utilisateurs, à l'image des sites de ventes aux enchères en ligne pour lesquels le catalogue des interdictions s'est élargi au fil du temps.

3. Titularité des droits sur les prompts et données d'entraînement (input)

On assimilera ici les prompts aux données ingérées («Input») dans le modèle aux fins de l'entraîner pour atteindre le but visé. La question se pose de savoir si ces Input sont propres au client, s'ils sont acquis auprès de tiers ou s'il s'agit de données publiques collectées sur le net. Chaque constellation conduit à des réflexions différentes.

a) Données propres du client

À supposer que les Input appartiennent au client, ce dernier s'assurera tout d'abord que leur ingestion dans le modèle ne conduit pas à conférer une licence en faveur du fournisseur allant au-delà de ce qui est nécessaire pour la bonne exécution du contrat, notamment en lui concédant un droit d'utiliser par la suite ces Input pour entraîner son modèle. La plupart des fournisseurs d'outils génératifs ont aujourd'hui compris que le succès commercial passe par l'octroi de garanties aux clients que leurs données ne seront pas utilisées pour entraîner leurs modèles; si la vigilance demeure de mise, une tendance favorable aux clients semble ainsi se dessiner en la matière.

Du côté du fournisseur, à partir du moment où il n'a pas de moyen de contrôle sur les prompts ou données d'entraînement ingérées par le client, il est légitime qu'il puisse exiger une garantie d'absence de violation des droits de tiers de la part du client, respectivement prévoir une obligation d'être indemnisé pour tout préjudice qui pourrait résulter pour lui de la violation d'une telle garantie.

b) Données de tiers

Lorsque le client acquiert des sets de données de tiers, le faisceau contractuel s'élargit, puisque le client aura en sus du contrat de licence auquel il souscrit pour utiliser l'outil standard autant de contrats que nécessaires avec les titulaires desdits sets de données.

S'agissant de ce second contrat, le client devra tout d'abord veiller que les droits qui lui sont conférés par le donneur de licence lui permettent d'atteindre l'objectif visé. À cet égard, il devra en particulier faire attention aux restrictions susceptibles d'exister quant à son droit d'agréger les données, les étiqueter, les nettoyer, les compiler et l'obligation qui pourrait lui être faite de détruire ces sets à l'expiration de la licence, une obligation sur la faisabilité technique de laquelle le client aura tout intérêt à s'interroger avant qu'il ne soit trop tard.

Le client devra ensuite s'assurer que le donneur de licence garantit que les sets de données (ou prompts retravaillés et suggérés) ne violent pas les droits de tiers, notamment d'auteur, et qu'il l'indemnisera de tout préjudice résultant de la violation d'une telle garantie.

Il devra enfin s'assurer qu'il est en droit de concéder une sous-licence au fournisseur de l'outil, dans la mesure nécessaire à l'ingestion des données aux fins d'entraîner le modèle.

Quant au fournisseur de l'outil, peu lui importe que les données ingérées soient celles du client ou d'un tiers. Dans

1 ‹https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/›.
2 ‹www.cnil.fr/fr/ia-comment-se-mettre-en-conformite›.
3 ‹www.cnil.fr/fr/realiser-une-analyse-dimpact-si-necessaire›.
4 Pour un ouvrage de référence en la matière: F. Marengo, Privacy and AI, 2023.

un cas comme dans l'autre, à partir du moment où il n'a pas de pouvoir de contrôle sur ces données, l'octroi en sa faveur d'une garantie d'absence de violation de droits et indemnisation y relative apparaissent légitimes.

c) Données publiques

Le client peut enfin entraîner le modèle au moyen de données collectées sur le net *(scraping)*. En dehors des aspects contractuels, le client devrait s'interroger sur le caractère licite d'un tel procédé eu égard aux données qu'il entend collecter. À cet égard, les États-Unis et l'Union européenne ont opté pour une approche libérale. *Van Buren v. United States*[5] et *hiQ Labs.v Linkedin*[6] semblent valider ce procédé aux Etats-Unis en ce qui a trait aux données publiquement accessibles, même si le Tribunal fédéral du district de Caroline du Nord a nuancé ces jurisprudences dans l'arrêt *Meta v. Brandtotal Ltd*[7] en considérant que cette dernière avait violé les conditions générales de Meta interdisant le recours à un tel procédé. Au sein de l'Union européenne, en une veine similaire à celle qui se dessine aux Etats-Unis, l'art. 4 de la Directive 2019/790 admet un tel procédé pour autant qu'il n'ait pas été interdit à la source par des mesures prises à cet effet (comme l'insertion d'une clause dans des conditions générales à l'image de Meta). Force est d'admettre que la situation en Suisse est plus complexe, et que seul le droit de la concurrence déloyale, en particulier les art. 2 et 5 lit. c LCD, à l'application délicate, pourrait offrir une aide contre le recours à un tel procédé pour des données publiques librement accessibles; demeure il est vrai réservée la délicate question du respect des réglementations applicables en matière de protection des données susceptibles d'être mises à mal par un tel procédé, comme en témoigne la déclaration conjointe émise par dix autorités nationales de protection en matière de données au mois d'août 2023, dont la Suisse.[8]

Quoi qu'il en soit, au vu de ces incertitudes, le fournisseur exigera de la part du client qui recourt à un tel procédé qu'il lui garantisse agir conformément à la réglementation applicable et qu'il ne viole aucun droit de tiers, respectivement qu'il l'indemnise s'il viole cette garantie.

La réciproque peut également exister lorsque le fournisseur recourt à un tel procédé pour fournir à ses clients un modèle entraîné, l'exemple type étant les LLMs. En cette hypothèse, il serait de bon ton que les clients puissent exiger une garantie de conformité et d'absence de violation de droits, que les fournisseurs sont assurément peu enclins à fournir en dépit d'un discours officiel se voulant rassurant.

4. Titularité des droits sur le résultat (output)

Pendant des questions touchant à la titularité des droits sur les données d'entraînement, le client veillera plus particulièrement à ce qu'il détienne tout d'abord seul les droits sur le résultat de l'exploitation de l'outil et que, deuxièmement, le fournisseur ne se réserve pas en retour le droit d'utiliser ce résultat pour entraîner son modèle. Ces deux points sont aujourd'hui assez largement reconnus.

Le client souhaitera le plus souvent s'assurer que le résultat ne viole pas les droits de tiers et être là encore indemnisé en cas de violation de cette garantie. Fort logiquement, le fournisseur ne peut toutefois garantir que ce qu'il contrôle. À supposer que le modèle ait été entraîné avec des données du client ou d'un tiers sur lesquelles il n'a aucun moyen de contrôle, ou que l'outil repose lui-même sur un modèle préexistant dans le cadre du *AI stack*, le fournisseur ne pourra alors pas fournir une telle garantie allant au-delà de sa sphère de contrôle. Le risque devra alors être assumé par le client.

Sans entrer dans les détails, c'est ici également l'occasion de relever une problématique particulière pour les développeurs recourant à des outils génératifs pour développer du code informatique. À supposer que le LLM soit entraîné sur du code faisant l'objet d'une licence libre et qu'une partie de ce code se retrouve dans le résultat, il y a fort à parier que le code en résultant ne respectera pas les conditions des licences libres.

Parmi les difficultés rencontrées, on mentionnera tout d'abord l'attribution des droits (autrement dit le «*copyright notice*»). Difficile en effet de concevoir que cette attribution, obligatoire dans toute licence libre, aussi permissive soit-elle, puisse être respectée. Consciente de ces difficultés, la fondation Linux a adopté des «*Community Data License Agreement (CDLA)*»,[9] dont le CDLA-Permissive-2.0[10] ne fait plus de cette attribution des droits une exigence absolue.

D'autres difficultés résident dans le fait que certains bouts de code peuvent être soumis à des licences incompatibles, ou que le résultat se trouve contaminé par une licence virale comme la GPL, alors que le client souhaite exploiter son code sous une forme propriétaire. À ce jour, de nombreuses questions demeurent à résoudre sur ces thématiques.

5. Garanties

Outre les garanties d'absence de violation de droit susmentionnées, le client pourra, suivant la finalité recherchée, souhaiter obtenir de plus amples garanties.

Parmi celles-ci, on peut mentionner la volonté pour le client d'avoir certaines garanties quant au niveau de performance du modèle, à l'image d'un SLA pour du SaaS. Force est pour le moment d'admettre qu'il n'existe encore guère de benchmarks en ce qui a trait à des SLA sur des outils d'IA. On peut cependant mentionner certaines garanties spécifiques en ce qui a trait à la latence, soit le temps néces-

5 593 U.S. __ (2021), disponible à l'adresse suivante: ‹https://supreme.justia.com/cases/federal/us/593/19-783/›.
6 938 F.3d 985 (9th Cir. 2019), disponible à l'adresse suivante: ‹https://casetext.com/case/hiq-labs-inc-v-linkedin-corp-2›.
7 20-cv-07182-JCS (N.D. Cal. May. 27, 2022), disponible à l'adresse suivante: ‹https://casetext.com/case/meta-platforms-inc-v-brandtotal-ltd-7›.
8 ‹www.edoeb.admin.ch/edoeb/fr/home/kurzmeldungen/2023/20230824_datascraping.html›.
9 ‹https://cdla.dev/›.
10 ‹https://cdla.dev/permissive-2-0/›.

saire pour l'outil à récolter les données nécessaires pour répondre à une requête.

Autre garantie, importante, celle octroyée au client que l'outil est conforme à la réglementation, en particulier en ce qui a trait à la réglementation européenne sur l'intelligence artificielle. Cette garantie pourra s'avérer délicate à octroyer lorsque la qualification d'un outil comme un système à haut risque dépend de l'utilisation qu'en fait le client, en particulier s'agissant des «*frontier models*».

On peut penser que, dans les années à venir, ce type de garantie sera remplacée par l'assurance de répondre à certains standards internationaux comme les standards ISO. Outre le standard ISO/IEC 42001:2023 (systèmes de management de l'IA), on peut mentionner la norme ISO/IEC 23894 (IA – recommandation relative au management du risque), la série ISO/IEC 5259 (données), les normes ISO/IEC TS 12791 et IEEE 7003 sur les biais, ou encore la norme à venir ISO/IEC 27090 (cybersécurité). De nombreuses normes couvrant en partie les exigences de la Réglementation européenne sur l'IA existent donc d'ores et déjà. Comme l'a relevé la Commission Européenne dans un rapport d'analyse,[11] ces normes ne couvrent toutefois pas totalement les exigences attendues. On peut toutefois s'attendre à ce que les travaux se poursuivent pour fournir aux acteurs des normes satisfaisant à ces exigences. Il suffira alors de s'y référer dans les contrats, comme on le fait depuis de nombreuses années s'agissant des contrats cloud et la norme ISO 27001 par exemple.

6. Responsabilité

Compte tenu des risques liés à de tels outils, le fournisseur cherchera le plus souvent à s'exonérer de toute responsabilité dans toute la mesure du possible, à tout le moins à la cantonner de manière mesurable. Une telle exonération se justifie essentiellement en deux hypothèses: tout d'abord, lorsque le résultat est généré ensuite de données propres ingérées par le client ou sur la base de sets de données fournis par des tiers ou sur lesquelles le fournisseur n'a aucun contrôle; deuxièmement, lorsque le résultat est généré ensuite d'une violation des restrictions contractuelles posées quant à l'étendue de la licence (par exemple en contournant par une manipulation de prompts certaines limites posées par le fournisseur).

Étant admis le fait que c'est au client qu'il incombera de prouver que les conditions posées à la responsabilité du fournisseur sont remplies, il y a fort à parier qu'il devra largement supporter le risque lié au recours à des tels outils compte tenu des difficultés probatoires. Quand bien même une proposition de directive existe à l'échelon européen pour alléger le fardeau de la preuve en établissant certaines présomptions notamment quant au rapport de causalité,[12] elle ne concerne que le cadre délictuel. La question de savoir dans quelle mesure elle pourrait trouver à s'appliquer, ne serait-ce que par analogie, dans un cadre contractuel, demeure ouverte.

7. Fin du contrat et clauses diverses

À partir du moment où le recours à des outils IA, généralement dans le cloud, implique une externalisation de données, le client devra veiller à l'image de n'importe quel contrat cloud à ce que les données susceptibles d'avoir été enregistrées chez le fournisseur soient détruites après l'expiration du contrat. A supposer que le recours à un outil déterminé soit susceptible de créer une forme de «*lock in*» pour le client dont il lui serait difficile de s'affranchir, il sera bon de s'intéresser aux conséquences résultant de la fin du contrat et s'assurer qu'une migration peut aisément avoir lieu, le cas échéant avec le soutien du fournisseur.

Enfin, on n'oubliera pas de s'intéresser à d'autres clauses dont l'importance doit être soulignée, comme celles ayant trait à la confidentialité, la sécurité (où il conviendra de tenir compte de risques propres aux systèmes IA comme les attaques de «*prompt injections*», «*jailbreaking*», «*poisoning*», «*sponge attacks*», etc.), l'obligation faite d'aviser le client en cas d'incident ou de problème détecté à quelque stade du cycle de vie de l'outil que ce soit, ou encore la conservation des logs *(«audit trail»)*.

II. Développement propre

Il peut arriver que le client ne trouve pas sur le marché de modèle correspondant à ses attentes ou que le modèle en question nécessite une personnalisation plus poussée pour répondre à ses besoins.

En cette hypothèse, toutes les questions examinées précédemment demeurent valables, étant précisé que les enjeux autour de la titularité des données se poseront non seulement pour les données d'entraînement, mais également en ce qui a traits aux sets de données utilisés pour tester et valider le modèle entraîné.

Les enjeux suivants seront en revanche propres à ces développements:

1. Définitions

De manière à éviter toute ambigüité, il est recommandé de définir certains termes spécifiques à l'environnement de ces outils en sus des termes usuels que l'on peut rencontrer dans des contrats informatiques, comme, parmi les plus usuels:

- Les données d'entrée d'origine, soit les données utilisées en leur état à l'origine (en distinguant potentiellement celles utilisées pour l'entraînement du modèle ou à d'autres fins);
- Les sets de données entraînées (autrement dit une fois nettoyées, agrégées, compilées ou étiquetées et pourvues de métadonnées);

11 ‹https://publications.jrc.ec.europa.eu/repository/handle/JRC132833›.
12 ‹https://commission.europa.eu/document/f9ac0daf-baa3-4371-a760-810414ce4823_en?prefLang=fr›.

– Le modèle non entraîné;
– Le modèle entraîné;
– Les prompts (si l'on est en présence d'un outil génératif);
– Les résultats *(output)*, souvent plutôt qualifiés de «suggestions».

2. Titularité des droits sur le modèle

Il convient de distinguer suivant que l'on est en présence du modèle non entraîné ou du modèle entraîné.

Le modèle non entraîné utilisé sera un modèle préexistant, sur lequel un tiers (qui peut être le fournisseur ou une tierce partie) détient les droits. À ce titre, ce modèle non entraîné constitue ce qui est régulièrement qualifié dans les contrats de développement informatique du «*background IP*», autrement dit de la propriété intellectuelle préexistante.

Les droits sur le modèle entraîné, respectivement les poids paramétrés, qui constituent un développement propre et qui représentent une valeur considérable, devraient en revanche appartenir au client qui paye pour ce développement au titre de «*foreground IP*». Des discussions sont évidemment susceptibles d'avoir lieu quant à l'intérêt que peut représenter pour le développeur un modèle entraîné et l'éventuel octroi à tout le moins d'une licence en sa faveur sur ledit modèle si ce modèle entraîné présente pour lui un intérêt commercial, une question qui sera abordée sur un plan commercial notamment au regard de l'avantage commercial qu'un tel modèle peut présenter pour le client.

L'octroi de la titularité des droits sur le modèle entraîné en faveur du client ne fait toutefois de sens que si l'exploitation dudit modèle n'est pas dépendante du modèle de base non entraîné. À supposer qu'une telle dépendance existe, une question loin d'être évidente tant le modèle entraîné peut diverger du modèle non entraîné, l'octroi d'une licence perpétuelle sur le modèle non entraîné est alors nécessaire faute de quoi on voit difficilement comment le client pourrait exploiter le modèle entraîné.

En toute hypothèse, le client attendra de la part du développeur qu'il lui garantisse que le modèle non-entraîné ne viole pas les droits de tiers, respectivement qu'il dispose le cas échéant des licences nécessaires pour permettre au client de l'entraîner. La question de savoir si une telle garantie peut être octroyée sur le modèle entraîné pourra être plus délicate à accorder si le client a joué un rôle actif dans l'entraînement du modèle, notamment par les jeux de données utilisés.

3. Exploitation

Une fois le modèle entraîné, il est à mon sens important de prévoir une phase test, qualifiée en français de recette d'acceptation. Cette phase devrait avoir lieu en production, dans la mesure où la précision d'un modèle entraîné présentera souvent un écart significatif dans un environnement de développement et un environnement en production où les paramètres à prendre en considération seront beaucoup plus nombreux.

Lorsque le modèle entraîné ne sert qu'à des fins d'exploitation interne, aucun problème particulier ne devrait se poser.[13] Lorsqu'il est en revanche destiné à être commercialisé, le client attachera une attention particulière aux clauses de garantie, d'autant plus importantes.

Parmi celles-ci, le client voudra notamment s'assurer que d'éventuels bouts de code du modèle entraîné ne s'avéreraient pas être soumis à une licence libre de nature virale qui viendrait contaminer l'ensemble du modèle et obliger le client à le commercialiser sous une telle licence; l'examen détaillé des risques liés aux licences libres dans le cadre de projets IA, complexe, dépasse toutefois le cadre de cette contribution et mérite assurément des recherches plus poussées.

Plus encore, le client apparaîtra en cette hypothèse comme le développeur au sens de la Réglementation européenne sur l'intelligence artificielle, avec toutes les obligations qui en résultent, en particulier s'il s'agit d'un système considéré comme à haut risque ou d'un modèle général *(«frontier model»)*. Il devra alors répercuter ses obligations sur le développeur pour s'assurer qu'il est à même de satisfaire à ces diverses exigences et s'assurer de sa collaboration à ce sujet, idéalement sans frais supplémentaire.[14]

III. Conclusion

La contractualisation de projets IA exige quelques bons réflexes. Si la liste présentée ici ne prétend nullement être exhaustive et ne reflète pas nécessairement la complexité de certains projets où les intervenants sont multiples, on peut néanmoins dégager les points saillants suivants qui se retrouveront quel que soit le projet visé:

– Données personnelles: il conviendra autant que faire se peut de veiller à ce qu'aucune donnée personnelle ne soit traitée, sauf à devoir conclure un accord de traitement en matière de données; le recours à des techniques de confidentialité apportera souvent une aide utile;
– La titularité des droits sur les données: on distinguera ici les données d'entrées, auxquelles on peut assimiler les prompts, en envisageant l'hypothèse où ces données sont celles du client, d'un tiers ou des données publiques d'une part, des données de sortie ou résultats générés par l'outil d'autre part. Une tendance se dessine à reconnaître que ces données d'entrée et les résultats appartiennent au client et, corollairement, que le fournisseur s'interdit de les utiliser pour améliorer son modèle; encore faudra-t-il toutefois porter pour les outils standards un regard attentif à l'abonnement souscrit, puisque le fournisseur est sus-

13 On réservera cependant dans le cadre d'outils génératifs notamment les garanties quant à l'absence de violation de droits sur les résultats, ou certains niveaux de performance attendus.

14 On pourra ici s'inspirer des contrats d'achat standards mis sur pied par la Commission européenne le 29 septembre 2023, disponible à l'adresse ‹https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/eu-model-contractual-ai-clauses-pilot-procurements-ai?utm_source=pocket_saves›.

ceptible de se réserver un tel droit pour les versions gratuites;
- La titularité des droits sur les modèles lors de développements spécifiques: on distinguera les droits sur le modèle non entraîné, qui appartiennent à l'exploitant *(background IP)*, des droits sur le modèle entraîné et les poids paramétrés, sur lesquels le client voudra détenir la titularité *(foreground IP)*, avec d'éventuelles difficultés de négociation en cas de dépendance (souvent relative) du second vis-à-vis du premier;
- Les garanties: nombreuses seront les garanties touchant en particulier à l'absence de violation de droits de tiers, qu'elle émane du client en faveur du fournisseur en ce qui a trait aux sets de données sur lesquels le fournisseur n'a aucun contrôle, ou de la part du fournisseur vis-à-vis du client quant à l'absence de violation de droits sur son modèle et les clauses d'indemnisation qui en découlent. D'autres clauses de garantie, liées à la performance ou à la conformité à la réglementation légale seront également usuelles; on pense notamment à des réglementations de conformité visant des domaines spécifiques comme les domaines bancaire ou de la santé ou au Règlement européen sur l'IA ou, où la référence à des standards internationaux se dessinera assurément dans les années à venir.
- La responsabilité: le fournisseur cherchera bien souvent à s'exonérer largement de toute responsabilité, en la conditionnant en particulier au respect des conditions d'octroi de la licence. Le client prêtera alors une attention particulière aux clauses définissant les usages autorisés *(AUP, Acceptable Use Policy)* et les restrictions d'utilisation *(Usage Restrictions)*, dont la liste devrait s'étoffer au fil du temps.

S'il est trop tôt pour parler encore de bonnes pratiques, des tendances se dessinent peu à peu dans un marché en devenir. Nous espérons avoir ici contribué à apporter aux intervenants dans les projets IA une grille de lecture des clauses les plus usuelles.

Résumé

Les questions touchant à la contractualisation des projets impliquant le recours ou le développement de modèles d'intelligence artificielle sont encore nombreuses. S'il n'existe encore aucun véritable standard, certaines tendances se dessinent. La présente contribution s'efforce de dresser un tour d'horizon des réflexes à avoir en présence de contrats impliquant le recours à un outil standard ou au développement d'un modèle propre.

Sont ainsi tour à tour examinées les questions touchant à l'éventuel traitement de données personnelles lors du recours à ces outils, la titularité des droits sur les données d'entrées en distinguant suivant qu'elles proviennent du client, de tiers ou d'un environnement public en libre accès, la titularité des droits sur les résultats et les questions touchant aux clauses de garantie et de responsabilité sans oublier, pour les modèles entraînés, les enjeux autour de la titularité des droits sur le modèle lui-même et les questions touchant à l'exploitation de tels modèles entraînés.

Zusammenfassung

Es gibt noch viele offene Fragen in Bezug auf die Vertragsgestaltung bei Projekten mit Einsatz oder Entwicklung von KI-Modellen. Es existiert zwar noch kein wirklicher Standard, doch es zeichnen sich gewisse Tendenzen ab. Dieser Beitrag versucht, einen Überblick über die Überlegungen zu geben, die bei Verträgen mit Einsatz eines Standard-Tools oder Entwicklung eines eigenen Modells anzuwenden sind.

So werden der Reihe nach Fragen geprüft zur allfälligen Verarbeitung persönlicher Daten beim Einsatz dieser Tools, zu Rechten an den Eingabedaten, je nachdem, ob sie vom Kunden, Dritten oder einer frei zugänglichen öffentlichen Umgebung stammen, zu Rechten an den Ergebnissen und Fragen zu Garantie- und Haftungsklauseln, sowie für trainierte Modelle Fragen rund um die Rechte am Modell selbst und Fragen zur Nutzung solcher trainierter Modelle.