



Préserver le secret professionnel dans les enquêtes assistées par l'IA

Charles Goumaz, Benjamin Borsodi, Louis Burrus, Clara Gehner

Key Take-aways

1.

Le droit suisse ne prévoit aucune règle spécifique sur le secret professionnel en matière l'IA. La protection des résultats générés par l'IA dépend de leur rattachement à une analyse juridique dirigée par un avocat – une question que les tribunaux suisses n'ont pas encore tranchées.

2.

Plusieurs régimes imposent des limites quant aux modalités et aux lieux d'utilisation de l'IA : le secret professionnel, la protection des données et l'interdiction d'exécuter des actes pour un Etat étranger.

3.

La protection par le secret professionnel des résultats générés par l'IA se joue avant leur déploiement. Une gouvernance insuffisante expose les enquêtes à la divulgation.

1 Contexte

Les outils d'intelligence artificielle (**IA**) sont de plus en plus utilisés dans le cadre des **enquêtes internes** menées par les entreprises. L'IA accélère la revue des documents, détecte des schémas, extrait les informations pertinentes et génère rapidement des comptes rendus d'entretiens structurés. Ces gains sont particulièrement importants dans les enquêtes complexes et multi juridictionnelles.

Le recours à l'IA dans les enquêtes soulève toutefois des questions juridiques auxquelles le droit suisse n'apporte pas encore de réponse directe. La principale concerne le **secret professionnel de l'avocat**: lorsque des outils d'IA génèrent des résultats d'enquête – tels que des synthèses, des indicateurs de pertinence ou des retranscriptions d'entretiens – ces résultats sont-ils protégés contre leur divulgation aux autorités de poursuite pénale, aux autorités de surveillance ou aux parties adverses dans une procédure civile ? En l'état actuel du droit suisse, cette question n'a pas encore été tranchée.

2 Le secret professionnel de l'avocat externe : le critère déterminant

Le droit suisse protège le **secret professionnel de l'avocat** au moyen de plusieurs régimes qui se recoupent. En vertu de l'art. 321 du Code pénal (**CP**), l'avocat ou son auxiliaire commet une infraction pénale s'il révèle des informations confidentielles concernant son client. L'art. 13 de la loi sur la libre circulation des avocats (**LLCA**) prévoit que tout avocat admis à pratiquer en Suisse est tenu de garder secrets les faits qui lui ont été confiés par son client ou un client potentiel.

Sur le plan procédural, les art. 160, 163 et 166 du Code de procédure civile (**CPC**), les art. 171 et 264 du Code de procédure pénale (**CPP**), ainsi que les art. 13, 16 et 17 de la loi fédérale sur la procédure administrative (**PA**), confèrent tant aux parties qu'aux tiers le droit de refuser la production de pièces couvertes par le secret professionnel ; sur le même fondement, l'avocat et son client peuvent également refuser de témoigner sur des informations protégées.

La protection suppose un mandat juridique, la direction d'un avocat qualifié et l'exercice de son **activité professionnelle typique**, à savoir le conseil et la représentation juridiques de ses clients.

Les tribunaux suisses n'ont pas statué sur l'IA et le secret professionnel.

Il convient toutefois de rappeler que la jurisprudence récente du Tribunal fédéral a restreint la notion d'« activité typique » de l'avocat dans le contexte des enquêtes internes. Dans les enquêtes internes, la seule **collecte des faits** ne relève pas automatiquement de l'activité typique de l'avocat.

C'est précisément sur ce point que se situe la principale difficulté des enquêtes assistées par l'intelligence artificielle. Aucune de ces dispositions n'a été conçue pour des résultats générés par l'IA. Le cadre législatif traite des communications entre l'avocat et le client – lettres, mémorandums, conseils, instructions. Il ne traite pas des résultats générés de manière autonome par une machine traitant les données du client sous la direction du conseil. Les tribunaux devront donc déterminer, par analogie avec les principes applicables au travail juridique humain, si ces résultats sont couverts par le secret professionnel.

Règle n° 1 – Formaliser un mandat juridique avant tout recours à l'IA.

La question déterminante n'est donc pas de savoir si le document a été produit par un être humain ou par une IA, mais qui a donné instruction d'utiliser l'outil, en quelle qualité et dans quel but. Lorsqu'un avocat recourt, dans le cadre d'un mandat formel, à une plateforme d'analyse assistée par l'IA pour conduire une enquête interne, et que les données sont traitées **sous sa direction**, les résultats produits peuvent être considérés comme le fruit du travail de l'avocat. L'IA n'agit alors que comme un instrument de l'avocat.

Cette protection suppose toutefois le maintien de la confidentialité. Le fournisseur doit pouvoir être qualifié d'auxiliaire de l'avocat, être lié contractuellement au secret professionnel et empêché d'accéder aux données ou de les réutiliser, ou l'outil doit fonctionner dans un environnement fermé. Une plateforme publique ne répondra généralement pas à ces exigences.

En revanche, lorsqu'un service de *compliance*, les ressources humaines ou un dirigeant utilise un outil d'IA hors de tout mandat juridique, les résultats ne sont pas protégés par le secret professionnel.

3 Le nouveau secret professionnel des juristes d'entreprise: plus limité qu'il n'y paraît

Entré en vigueur le 1er janvier 2025, le CPC révisé a introduit un **secret professionnel limité** en faveur des juristes d'entreprise à l'art. 167a CPC. Cette protection est subordonnée à trois conditions cumulatives. Premièrement, la personne morale qui invoque le secret doit être inscrite au registre du commerce. Deuxièmement, le service juridique interne doit être dirigé par un avocat admis à exercer en Suisse ou dans son État d'origine. Troisièmement – et c'est l'élément le plus déterminant dans le contexte des enquêtes assistées par l'IA – l'activité concernée doit relever de l'activité typique de l'avocat, à savoir le conseil et la représentation juridiques.

Deux limites importantes doivent toutefois être soulignées.

Premièrement, ce nouveau secret professionnel ne s'applique qu'aux **procédures civiles**. Il n'offre aucune protection dans les procédures pénales régies par le CPP, ni dans les procédures administratives menées par la FINMA ou d'autres autorités de surveillance. Il s'agit d'une limitation fondamentale : l'art. 167a CPC ne protège pas les entreprises dans les enquêtes les plus sensibles.

Deuxièmement, la **définition de l'« activité typique »** du juriste d'entreprise demeure controversée en jurisprudence. Les tribunaux ont indiqué que les tâches opérationnelles, les activités de conformité ainsi que certaines opérations de collecte des faits dans le cadre d'enquêtes internes ne relèvent pas nécessairement de cette activité. Ainsi, lorsqu'un juriste d'entreprise utilise un outil d'IA pour classer des documents ou analyser des comportements potentiellement illicites, mais que les résultats sont ensuite exploités principalement par les fonctions de conformité ou la direction à des fins opérationnelles plutôt que pour préparer un avis juridique, le lien avec une activité protégée par le secret professionnel s'en trouve affaibli.

Afin d'éviter la création de documents d'analyse détaillés mais dépourvus de protection, les entreprises suisses doivent mettre en place et faire respecter des directives internes claires. Celles-ci doivent prévoir que les outils d'IA ne peuvent traiter des données liées à une enquête que dans le cadre d'un processus approuvé et placé sous la direction d'un conseiller juridique. Cette exigence vaut aussi bien pour les outils d'IA grand public utilisés via des comptes personnels que pour les plateformes mises à disposition par l'entreprise.

Règle n° 2 – Former les collaborateurs aux usages interdits de l'IA.

4 La LPD : les fournisseurs d'IA en tant que sous-traitants

En vertu de la loi fédérale révisée sur la protection des données (**LPD**), le **traitement de données d'enquête par un fournisseur tiers d'IA** constitue une communication de données à un sous-traitant. Cette qualification entraîne deux obligations dont la violation peut compromettre le secret professionnel.

La première obligation consiste à conclure avec le fournisseur d'IA un **contrat de sous-traitance** définissant notamment les finalités du traitement, les mesures de sécurité applicables et, surtout, la possibilité ou non pour le fournisseur d'utiliser les données du client afin d'entraîner ou d'améliorer ses modèles. Si le fournisseur exploite les données de l'enquête à cette fin, cela peut constituer une violation du secret professionnel et compromettre, voire faire perdre, la protection qui en découle.

La seconde obligation consiste à **limiter les transferts de données personnelles vers des États ne garantissant pas un niveau de protection adéquat**, sauf si des garanties appropriées sont mises en place. Le

transfert de données vers des systèmes d'IA hébergés hors de Suisse suppose soit une décision d'adéquation couvrant le destinataire, soit des garanties appropriées, telles que des clauses contractuelles types (*Standard Contractual Clauses*) adaptées au droit suisse.

Depuis le 15 septembre 2024, les États-Unis bénéficient d'une décision suisse d'adéquation, mais uniquement pour les fournisseurs auto-certifiés dans le cadre du *Swiss-U.S. Data Privacy Framework (DPF)*. Pour les autres, des SCC adaptées au droit suisse demeurent indispensables. Cette décision d'adéquation ne dispense toutefois pas de l'évaluation de l'accès potentiel des autorités étrangères aux données lorsque celles-ci sont couvertes par le secret professionnel. En d'autres termes, le recours à un fournisseur américain certifié DPF ne suffit pas, à lui seul, à résoudre les problématiques de localisation des données examinées ci-après.

Règle n° 3 – Exiger des fournisseurs d'IA des garanties contractuelles renforcées.

Une équipe d'enquête qui télécharge sur une plateforme d'IA hébergée aux États-Unis des communications d'employés, des dossiers de ressources humaines ou des données transactionnelles sans mécanisme de transfert conforme à la LPD s'expose ainsi à une violation de cette loi. Une telle communication, en dehors du canal protégé par le secret professionnel, peut finalement priver l'équipe de la protection même qu'elle cherchait à préserver.

5 L'« interdiction d'exécuter des actes pour un État étranger » : la localisation des données comme contrainte impérative

L'art. 271 CP interdit d'accomplir ou de faciliter, sur le territoire suisse, des **actes pour le compte d'un État étranger** qui relèvent, selon le droit suisse, des autorités publiques, sauf autorisation préalable de la Confédération. En outre, l'art. 273 CP interdit la communication de secrets d'affaires ou de fabrication à un État étranger, tandis que l'art. 162 CP réprime la divulgation de secrets d'affaires de tiers en violation d'une obligation légale ou contractuelle de confidentialité.

Ces dispositions peuvent trouver application lorsqu'une entreprise transfère à un fournisseur étranger d'IA des données d'enquête, telles que des informations relatives à ses clients, à sa stratégie commerciale ou à ses opérations. L'art. 271 CP a déjà été appliqué à des avocats ayant remis des documents situés en Suisse à des autorités étrangères en dehors des voies officielles d'entraide.

Le stockage ou le traitement de données d'enquête suisses sur une plateforme d'IA hébergée dans le cloud

dont les serveurs se trouvent aux États-Unis expose ces données à un accès contraignant par les autorités américaines, notamment en vertu du *US Cloud Act*. Le stockage de données d'enquête sur des serveurs américains peut exposer celles-ci à un accès des autorités étrangères, avec un risque d'application des art. 271 et 273 CP.

Règle n° 4 – Héberger les données d'enquête en Suisse en cas de risque transfrontalier.

Le risque est particulièrement élevé dans les enquêtes présentant une dimension américaine, notamment lorsqu'elles impliquent le *Department of Justice (DOJ)* ou l'*Office of Foreign Assets Control (OFAC)*, compte tenu de la portée extraterritoriale des pouvoirs de ces autorités. Les données concernées devraient être stockées et traitées exclusivement en Suisse.

6 Conclusion

Le recours aux outils d'intelligence artificielle dans les enquêtes internes offre des avantages considérables. La véritable question n'est donc plus de savoir s'il faut utiliser ces outils, mais s'ils sont déployés dans un cadre juridique permettant de préserver les protections qui garantissent l'efficacité et la sécurité de l'enquête.

L'analyse conduit à une conclusion claire : la protection par le secret professionnel des résultats d'enquête générés par l'IA dépend presque entièrement des **décisions prises avant même l'activation des outils**. La mise en place d'une gouvernance préalable est déterminante. Le recours précoce à un avocat, le choix de fournisseurs conformes, l'hébergement des données en Suisse et l'interdiction de tout usage autonome de l'IA en constituent les principaux éléments.

Les entreprises qui investissent dans ce cadre de gouvernance pourront tirer pleinement parti des outils d'IA tout en préservant le bénéfice du secret professionnel. Celles qui s'en abstiennent risquent, dans les circonstances les plus défavorables, de devoir expliquer pourquoi les principaux résultats de leur enquête ne bénéficient d'aucune protection.



Charles Goumaz
Partner, Geneva
Charles.Goumaz@swlegal.ch



Benjamin Borsodi
Partner, Geneva
Benjamin.Borsodi@swlegal.ch



Peter Burckhardt
Partner, Zurich
Peter.Burckhardt@swlegal.ch



Simone Nadelhofer
Partner, Zurich
Simone.Nadelhofer@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.com

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

Singapour
Schellenberg Wittmer Pte Ltd
50 Raffles Place, #40-05
Singapore Land Tower
Singapore 048623
www.swlegal.sg