SCALE|AI

par **Todd Bailey**
VP, propriété intellectuelle et affaires juridiques

Guide : Protéger les secrets et les données

Secrets commerciaux, renseignements commerciaux de nature exclusive et renseignements confidentiels : ces termes sont pratiquement synonymes. Tous comportent l'idée de confidentialité et d'accès contrôlé.

La protection des secrets est peu coûteuse et ne nécessite pas d'enregistrements officiels, ce qui une option intéressante pour les startups. Mais c'est également la protection de PI la plus difficile à appliquer et à défendre en cour, car elle exige d'avoir de bonnes habitudes et de porter une attention quotidienne à la protection de ces secrets.

Un secret peut être fort ou faible. Ça dépendra de deux facteurs :

- si le propriétaire protège bien le secret
- et, de façon cruciale, s'il est facile d'établir par ingénierie inverse ou de développer de manière indépendante le secret; parce que s'il est possible de le découvrir, la façon dont il est protégé importe peu.

Des secrets forts nécessitent le bon type d'information et une protection systématique.

Qu'est-ce qui peut être protégé?

Toute PI non publique (idée, renseignement ou donnée) peut être protégée en tant que secret. Les codes logiciels, les données, la sélection des hyperparamètres, la pondération des paramètres, les spécifications techniques, les documents d'exigences techniques et les prix, en sont quelques exemples.

Secrets qu'il est avantageux de protéger :

- renseignements compliqués, difficiles à établir par ingénierie inverse;
- divers ensembles de renseignements, comme le savoir-faire
- les idées que vous ne pouvez pas (ou ne voulez pas) breveter ou protéger à l'aide d'autres outils de PI;
- les données propriétaires.

Les secrets qu'il est moins avantageux de protéger :

- les idées simples ou celles qui peuvent être obtenues par ingénierie inverse. Les soi-disant recettes secrètes ne sont que des légendes marketing;
- la PI fondamentale (au cœur même de votre entreprise), parce que si quelqu'un d'autre la fait breveter, vous allez devoir arrêter de l'utiliser;
- les choses dont vous souhaitez conserver l'exclusivité, parce que la protection des secrets ne peut empêcher une découverte indépendante ou l'ingénierie inverse.

Comment protéger les secrets

La protection repose sur des mesures que l'on peut faire soi-même :

- ne les dites pas aux autres, à moins qu'ils aient besoin de le savoir;
- conservez-les dans un lieu sûr, dont l'accès est restreint;
- identifiez-les à l'aide de la mention « confidentiel »;

- divulguez-les uniquement après la signature d'une entente de confidentialité.

Parmi les meilleures pratiques, notons également la tenue d'un registre de ce qui est divulgué (afin que vous puissiez plus tard prouver ce que vous aviez divulgué) et d'exiger que tout soit effacé ou retourné à l'expiration de l'entente de confidentialité.

a) Ne les dites pas aux autres

Les secrets sont à risque chaque fois que vous les divulguez à d'autres. Plus il y a de gens qui connaissent votre secret, plus il y a de risques de fuite.

Alors, plus votre secret est important, moins il doit y avoir de gens qui sont en mesure d'y accéder, et uniquement lorsqu'ils ont véritablement besoin de les savoir.

Les clients peuvent facilement devenir des concurrents. Donc, moins ils en savent, mieux c'est. Apprenez à parler de **ce que vous faites, et non de la façon dont vous le faites**. N'ayez pas peur de garder votre boîte noire fermée. La même chose s'applique dans vos discussions avec des investisseurs.

Les fournisseurs peuvent devenir des points de fuite. Concevez vos logiciels et processus de manière à ne pas avoir à divulguer vos secrets aux fournisseurs. **Gardez les choses importantes à l'interne**, et externalisez les choses courantes.

Les employés constituent également un risque. Oui, ils sont une ressource de confiance – mais ils peuvent également vous quitter pour devenir des concurrents. **Apprenez à isoler l'information à l'interne**, sur la base du besoin de connaître, de manière à ce que vos secrets importants ne franchissent pas votre porte chaque fois que des employés vous quittent.

Méfiez-vous des entreprises conjointes et partenariats qui pourraient être simplement un **stratagème pour avoir accès à vos secrets.** Comme avec les clients, parlez de ce que vous faites, mais pas de la façon dont vous le faites.

b) Conservez-les dans un lieu sûr, dont l'accès est restreint

C'est là où la plupart des gens sont leur pire ennemi. Le plus difficile avec les secrets, ce sont les habitudes quotidiennes nécessaires afin de préserver la protection légale.

Le système légal vous permettra uniquement de protéger en tant que secret **ce que vous protégez vraiment en tant que secret**. Pour faire valoir votre droit au secret devant les tribunaux, vous devez prouver que vous avez pris les mesures raisonnables pour protéger vos secrets. Bien plus de secrets sont perdus en raison d'une mauvaise gestion que de gestes malveillants.

Quelques pratiques exemplaires :

- le catalogage des secrets les plus importants;
- des contrôles physiques et électroniques appropriés pour restreindre l'accès, même à l'interne;
- des contrôles internes pour faire en sorte que des ententes de confidentialité soient signées avant toute divulgation;
- la protection des modèles, par exemple en les répartissant sur plusieurs serveurs;
- la conservation du code secret sur votre plateforme; faites en sorte que les modèles accèdent aux données au moyen d'interfaces API, sans divulgation du code source.

c) Identifiez-les à l'aide de la mention « confidentiel »

Les en-têtes des codes sources, les modèles de document et d'autres éléments secrets doivent porter des mentions de confidentialité pour avertir les autres, à l'interne et à l'externe, que cette information est votre secret.

d) Ententes de confidentialité

Si vous devez divulguer des secrets, il est nécessaire de faire **d'abord** signer une entente de confidentialité.

Les ententes de confidentialité ne sont pas toutes identiques – unidirectionnelles, bidirectionnelles, réciproques, limitées, perpétuelles –, il en existe de nombreux types et ne pas utiliser celle qui convient pourrait s'avérer fatal pour vos secrets.

Ne présumez pas que le modèle que vous avez téléchargé sur Internet ou copié d'un fournisseur est un bon modèle pour votre entreprise. Demandez plutôt à un avocat qui comprend votre entreprise de **préparer un modèle qui convient**. Et lorsque vous utilisez le modèle, n'acceptez pas de le modifier sans bien comprendre les répercussions sur vos secrets.

Même avec une entente de confidentialité signée, vous devez continuer d'appliquer le principe de « besoin de connaître » pour vous guider dans ce que vous divulguerez :

- Parlez de ce que vous faites, mais pas de la façon dont vous le faites.
- Parlez en termes **d'avantages utilisateur**, sans ouvrir votre boîte noire.
- Si vous devez ouvrir votre boîte noire, ouvrez-la le moins grand possible et ne **donnez à personne toutes les pièces de votre puzzle**.

Protéger les données

Ces principes s'appliquent également à la protection des données :

Protégez-les à l'aide de chiffrement ou d'un autre moyen; restreignez-en l'accès en utilisant le principe de « besoin de connaître »; les ententes de confidentialité sont essentielles; n'autorisez pas que des copies soient faites; et révoquez l'accès dès qu'il n'est plus nécessaire.

Si des données dérivées sont créées, leur propriété et leur accès devront être détaillés dans un contrat. Nous aborderons les contrats dans un prochain épisode de *Pourquoi la PI*